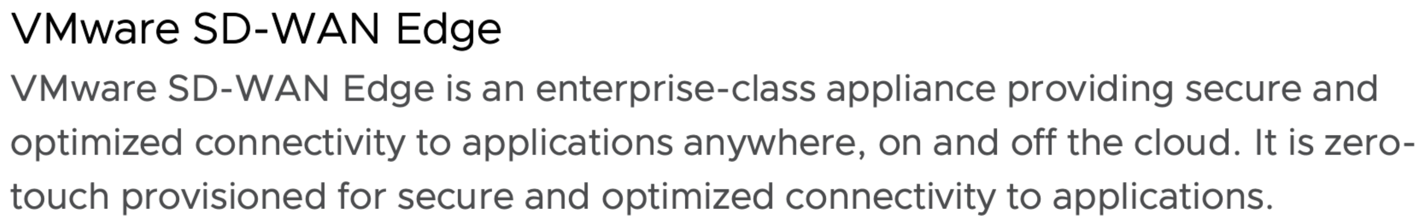
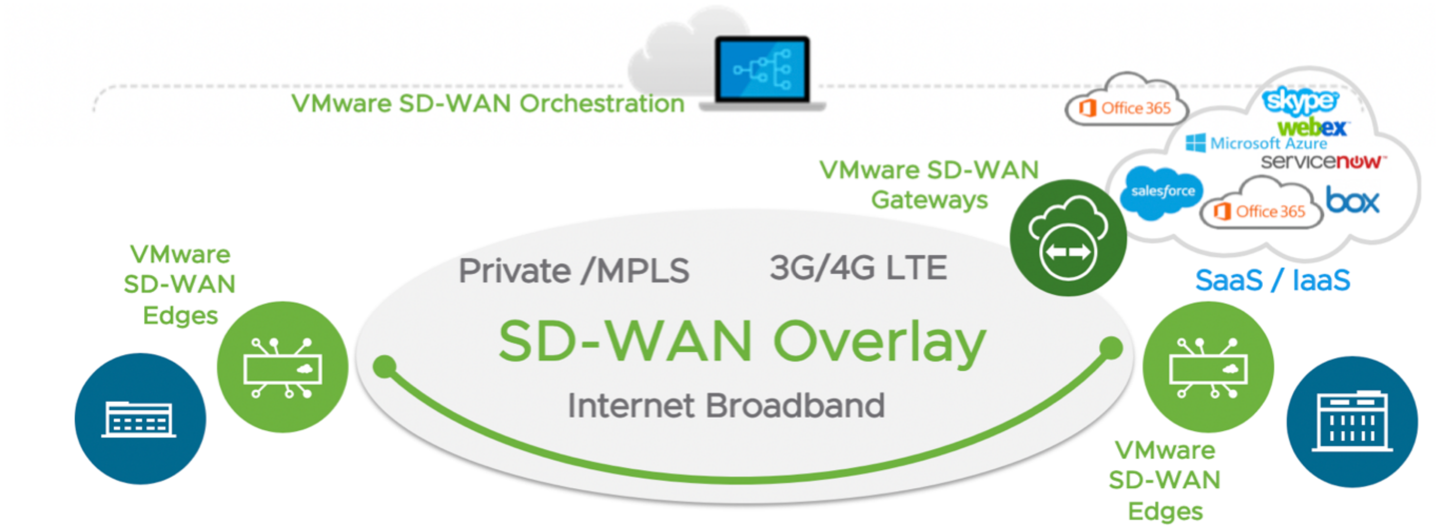
Exhibit 2

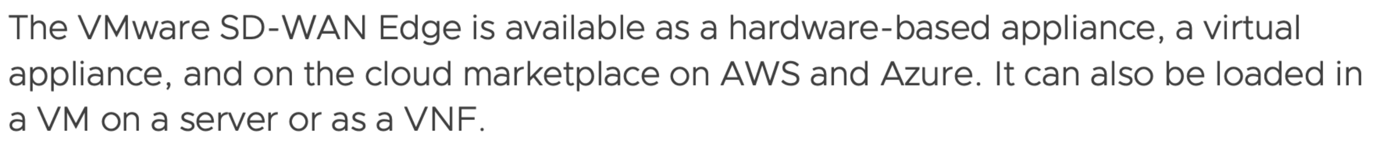
CHART FOR U.S. PATENT NO. 7,623,518 (“the ’518 Patent”)

Accused Products: VMware products, including at least each of the following appliances and software infringe at least Claim 15 of the ’518 Patent: VMware SD-WAN Edge 510, Edge 510 LTE, Edge 520, Edge 540, Edge 6x0, Edge 840, Edge 2000, Edge 3x00.

Claims	Exemplary Infringement Evidence
[15pre] A network switching circuit, comprising:	To the extent the preamble is limiting, each Accused Product comprises a network switching circuit.  VMware SD-WAN Edge VMware SD-WAN Edge is an enterprise-class appliance providing secure and optimized connectivity to applications anywhere, on and off the cloud. It is zero-touch provisioned for secure and optimized connectivity to applications. *See* https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-712-edge-platform-spec-ds-1020.pdf

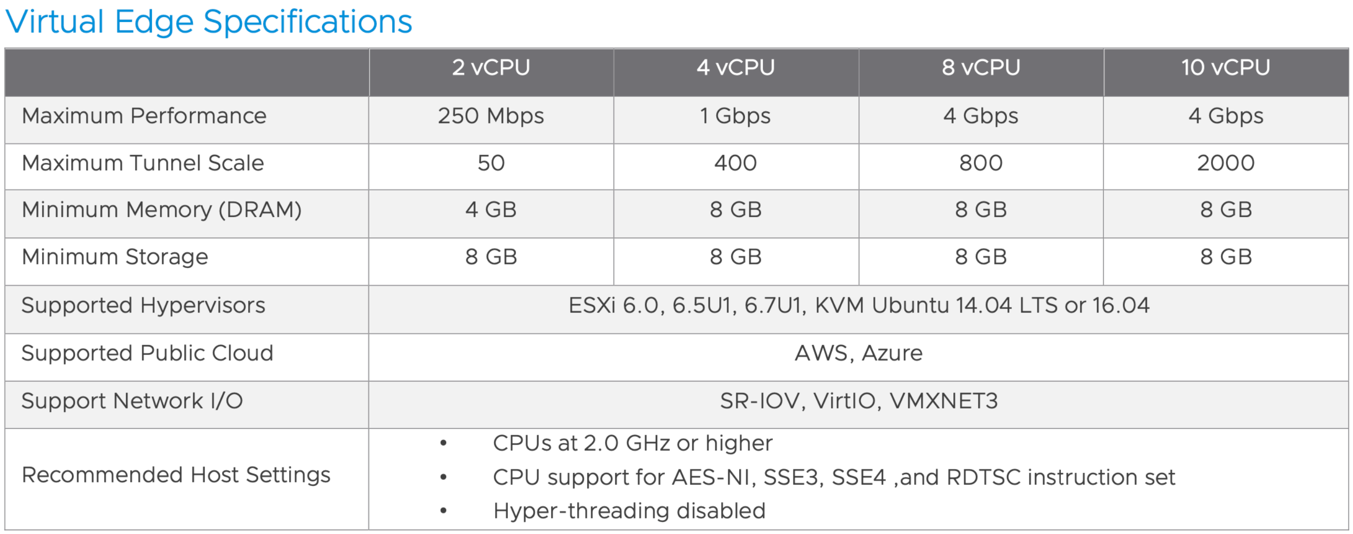
Claims	Exemplary Infringement Evidence
	 VMware SD-WAN Orchestration Office 365 skype webex Microsoft Azure servicenow salesforce Office 365 box VMware SD-WAN Gateways SaaS / IaaS VMware SD-WAN Edges Private /MPLS 3G/4G LTE SD-WAN Overlay Internet Broadband VMware SD-WAN Edges *Figure 1 VMware SD-WAN by VeloCloud* *See* VMware SD-WANTM by VeloCloud at p. 2.

Claims	Exemplary Infringement Evidence



The VMware SD-WAN Edge is available as a hardware-based appliance, a virtual appliance, and on the cloud marketplace on AWS and Azure. It can also be loaded in a VM on a server or as a VNF.

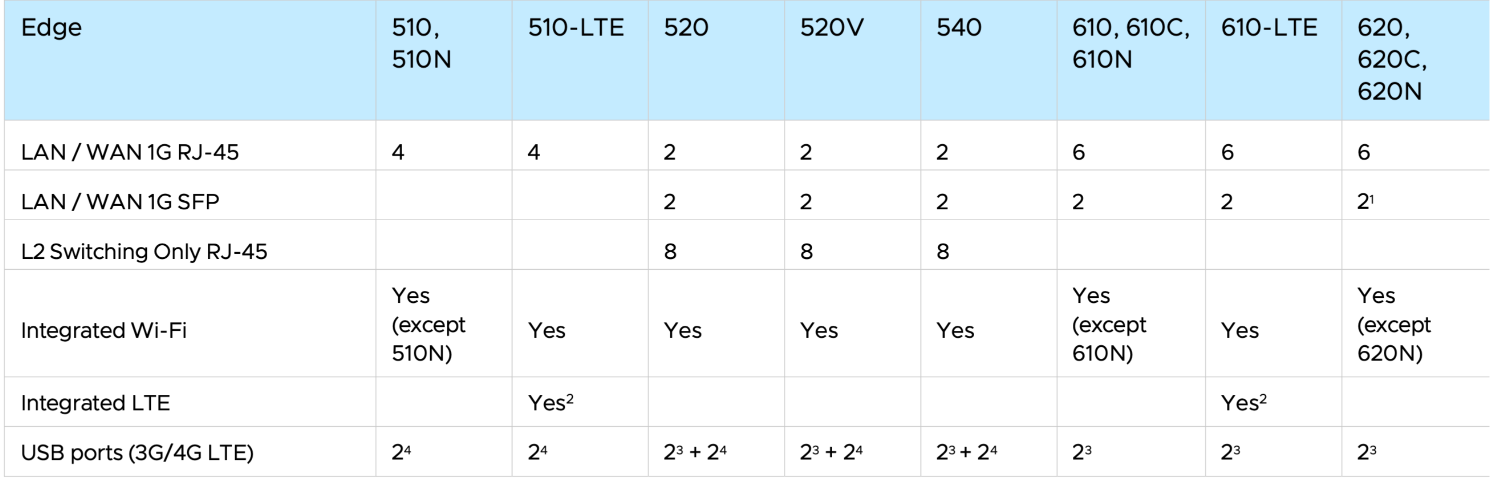
See VMware SD-WANTM by VeloCloud at p. 1.

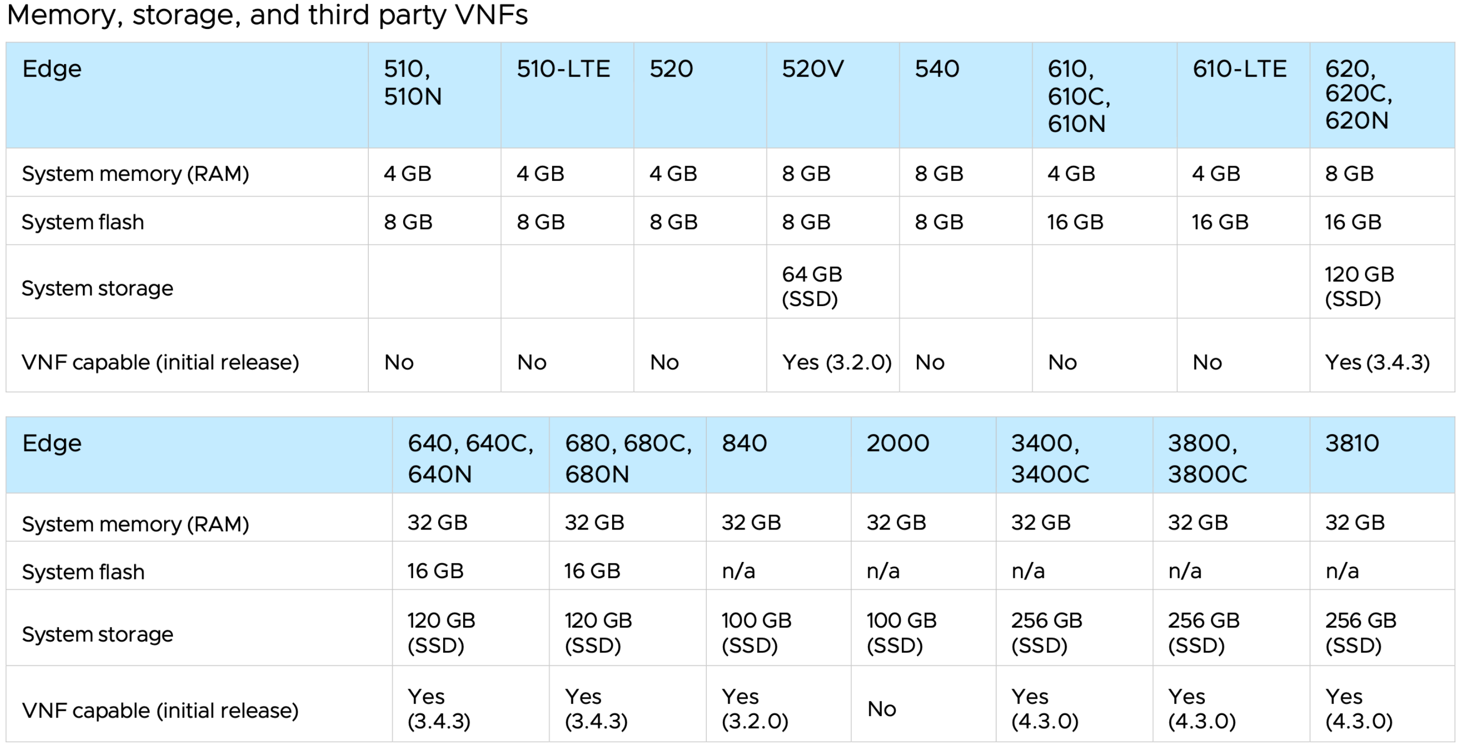


Virtual Edge Specifications

	2 vCPU	4 vCPU	8 vCPU	10 vCPU
Maximum Performance	250 Mbps	1 Gbps	4 Gbps	4 Gbps
Maximum Tunnel Scale	50	400	800	2000
Minimum Memory (DRAM)	4 GB	8 GB	8 GB	8 GB
Minimum Storage	8 GB	8 GB	8 GB	8 GB
Supported Hypervisors	ESXi 6.0, 6.5U1, 6.7U1, KVM Ubuntu 14.04 LTS or 16.04			
Supported Public Cloud	AWS, Azure			
Support Network I/O	SR-IOV, VirtIO, VMXNET3			
Recommended Host Settings	• CPUs at 2.0 GHz or higher • CPU support for AES-NI, SSE3, SSE4 ,and RDTSC instruction set • Hyper-threading disabled			

See VMware SD-WANTM by VeloCloud at p. 7.

<table>
<tr><th>Claims</th><th>Exemplary Infringement Evidence</th></tr>
<tr><td></td><td>

<table>
<tr><th>Edge</th><th>510, 510N</th><th>510-LTE</th><th>520</th><th>520V</th><th>540</th><th>610, 610C, 610N</th><th>610-LTE</th><th>620, 620C, 620N</th></tr>
<tr><td>LAN / WAN 1G RJ-45</td><td>4</td><td>4</td><td>2</td><td>2</td><td>2</td><td>6</td><td>6</td><td>6</td></tr>
<tr><td>LAN / WAN 1G SFP</td><td></td><td></td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2[1]</td></tr>
<tr><td>L2 Switching Only RJ-45</td><td></td><td></td><td>8</td><td>8</td><td>8</td><td></td><td></td><td></td></tr>
<tr><td>Integrated Wi-Fi</td><td>Yes (except 510N)</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes (except 610N)</td><td>Yes</td><td>Yes (except 620N)</td></tr>
<tr><td>Integrated LTE</td><td></td><td>Yes[2]</td><td></td><td></td><td></td><td></td><td>Yes[2]</td><td></td></tr>
<tr><td>USB ports (3G/4G LTE)</td><td>2[4]</td><td>2[4]</td><td>2[3] + 2[4]</td><td>2[3] + 2[4]</td><td>2[3] + 2[4]</td><td>2[3]</td><td>2[3]</td><td>2[3]</td></tr>
</table>
<i>See</i> https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-712-edge-platform-spec-ds-1020.pdf
</td></tr>
</table>

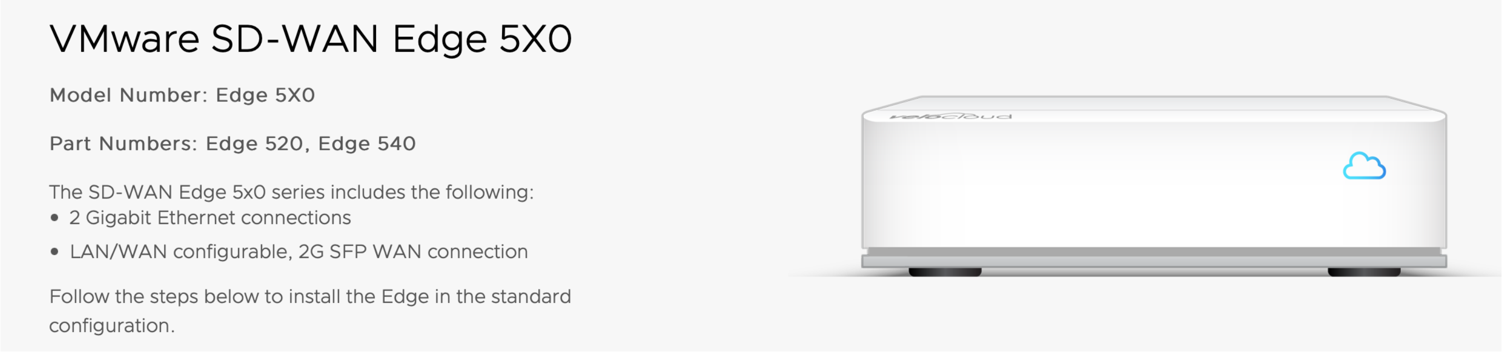
Claims	Exemplary Infringement Evidence
	

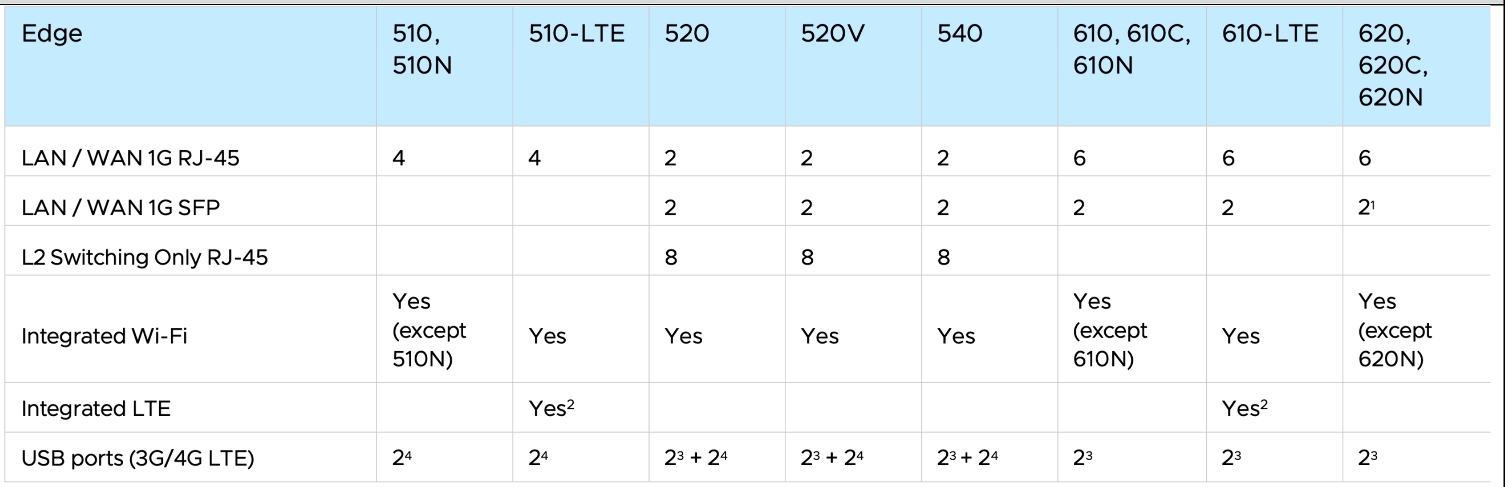
Memory, storage, and third party VNFs

Edge	510, 510N	510-LTE	520	520V	540	610, 610C, 610N	610-LTE	620, 620C, 620N
System memory (RAM)	4 GB	4 GB	4 GB	8 GB	8 GB	4 GB	4 GB	8 GB
System flash	8 GB	8 GB	8 GB	8 GB	8 GB	16 GB	16 GB	16 GB
System storage				64 GB (SSD)				120 GB (SSD)
VNF capable (initial release)	No	No	No	Yes (3.2.0)	No	No	No	Yes (3.4.3)

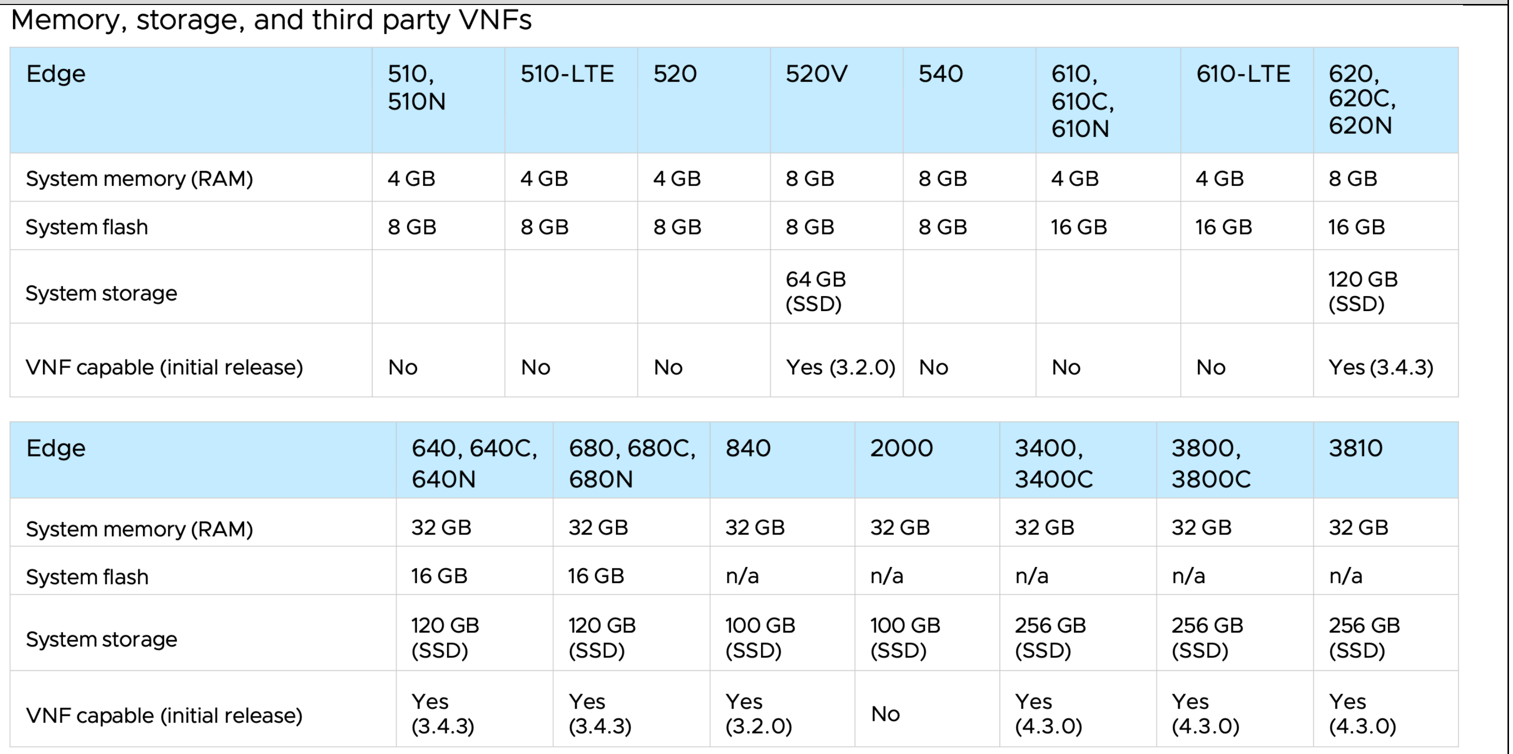
Edge	640, 640C, 640N	680, 680C, 680N	840	2000	3400, 3400C	3800, 3800C	3810
System memory (RAM)	32 GB	32 GB	32 GB	32 GB	32 GB	32 GB	32 GB
System flash	16 GB	16 GB	n/a	n/a	n/a	n/a	n/a
System storage	120 GB (SSD)	120 GB (SSD)	100 GB (SSD)	100 GB (SSD)	256 GB (SSD)	256 GB (SSD)	256 GB (SSD)
VNF capable (initial release)	Yes (3.4.3)	Yes (3.4.3)	Yes (3.2.0)	No	Yes (4.3.0)	Yes (4.3.0)	Yes (4.3.0)

See https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-712-edge-platform-spec-ds-1020.pdf

Claims	Exemplary Infringement Evidence
	 VMware SD-WAN Edge 5X0 Model Number: Edge 5X0 Part Numbers: Edge 520, Edge 540 The SD-WAN Edge 5x0 series includes the following: • 2 Gigabit Ethernet connections • LAN/WAN configurable, 2G SFP WAN connection Follow the steps below to install the Edge in the standard configuration. *See* https://sase.vmware.com/resources/edge-520
[15a] a forwarding circuit operable to detect specific received packets and to provide the specific packets on a processor port, and further operable to receive packets on one of a plurality of ports including the processor port and to forward each	Each Accused Product comprises a forwarding circuit operable to detect specific received packets and to provide the specific packets on a processor port, and further operable to receive packets on one of a plurality of ports including the processor port and to forward each received packet to a port corresponding to a destination address contained in the packet subject to access restrictions contained in a dynamic access control list.

<table>
<tr><th>Claims</th><th>Exemplary Infringement Evidence</th></tr>
<tr><td>received packet to a port corresponding to a destination address contained in the packet subject to access restrictions contained in a dynamic access control list;</td><td>

<table>
<tr><th>Edge</th><th>510, 510N</th><th>510-LTE</th><th>520</th><th>520V</th><th>540</th><th>610, 610C, 610N</th><th>610-LTE</th><th>620, 620C, 620N</th></tr>
<tr><td>LAN / WAN 1G RJ-45</td><td>4</td><td>4</td><td>2</td><td>2</td><td>2</td><td>6</td><td>6</td><td>6</td></tr>
<tr><td>LAN / WAN 1G SFP</td><td></td><td></td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2[1]</td></tr>
<tr><td>L2 Switching Only RJ-45</td><td></td><td></td><td>8</td><td>8</td><td>8</td><td></td><td></td><td></td></tr>
<tr><td>Integrated Wi-Fi</td><td>Yes (except 510N)</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes (except 610N)</td><td>Yes</td><td>Yes (except 620N)</td></tr>
<tr><td>Integrated LTE</td><td></td><td>Yes[2]</td><td></td><td></td><td></td><td></td><td>Yes[2]</td><td></td></tr>
<tr><td>USB ports (3G/4G LTE)</td><td>2[4]</td><td>2[4]</td><td>2[3] + 2[4]</td><td>2[3] + 2[4]</td><td>2[3] + 2[4]</td><td>2[3]</td><td>2[3]</td><td>2[3]</td></tr>
</table>
<i>See</i> https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-712-edge-platform-spec-ds-1020.pdf
</td></tr>
</table>

Claims	Exemplary Infringement Evidence

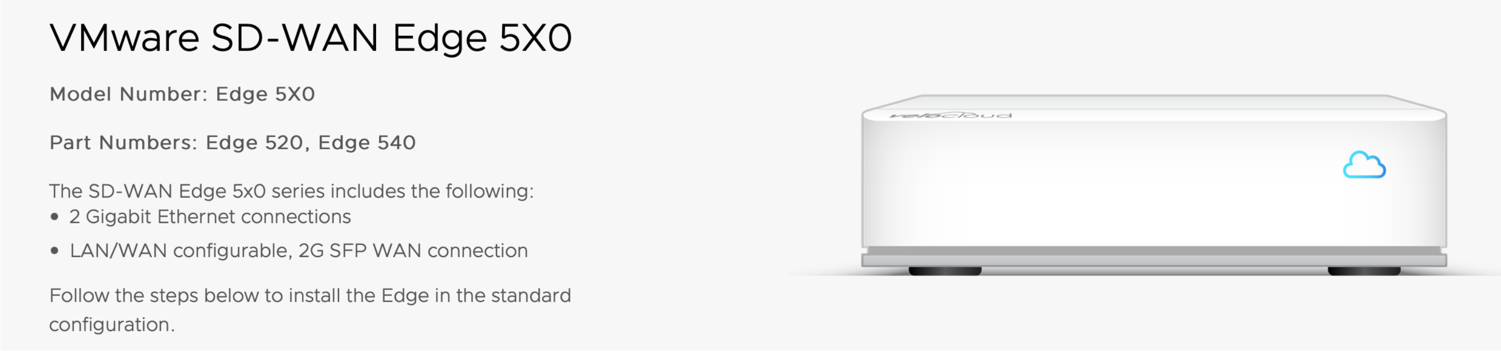
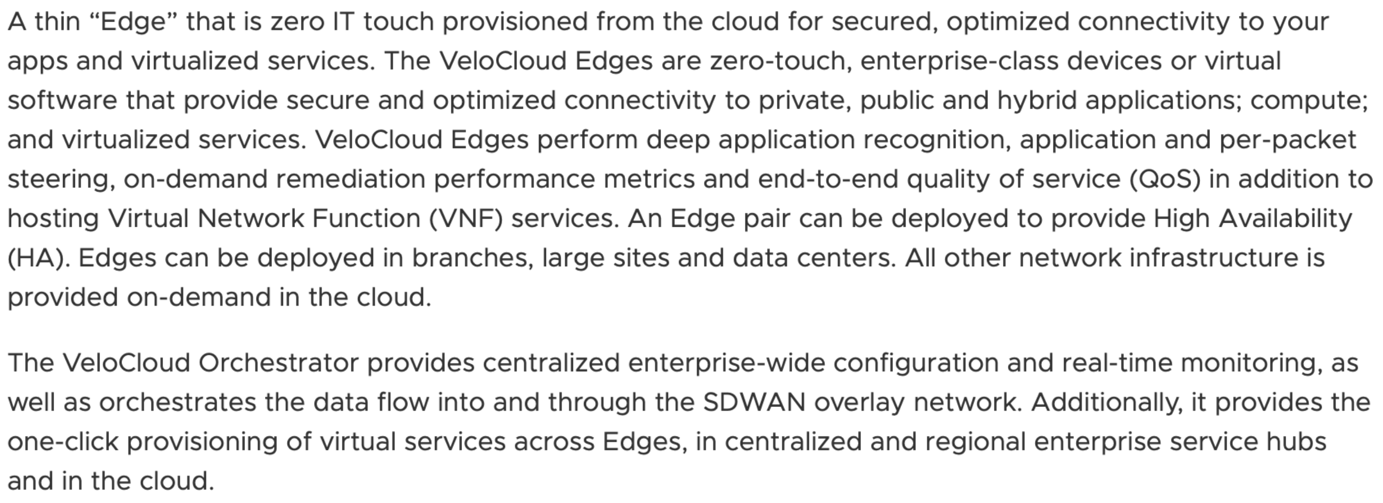


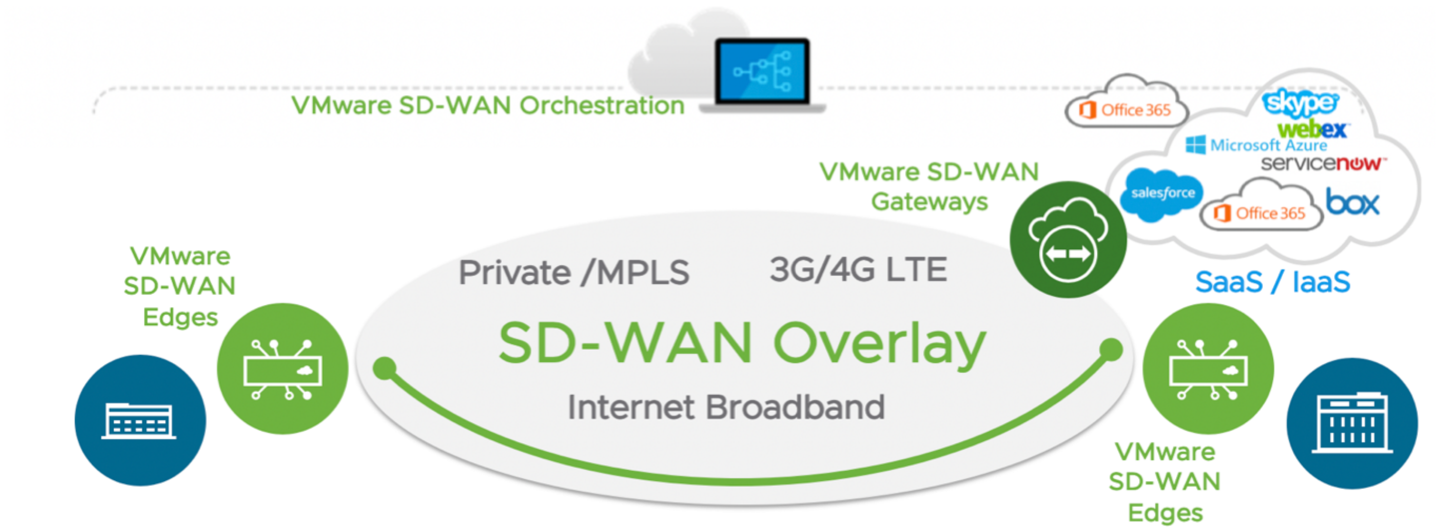
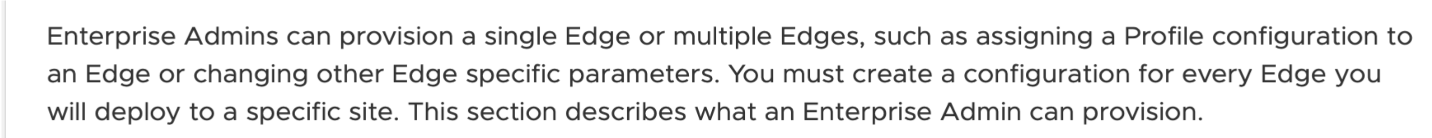
Memory, storage, and third party VNFs

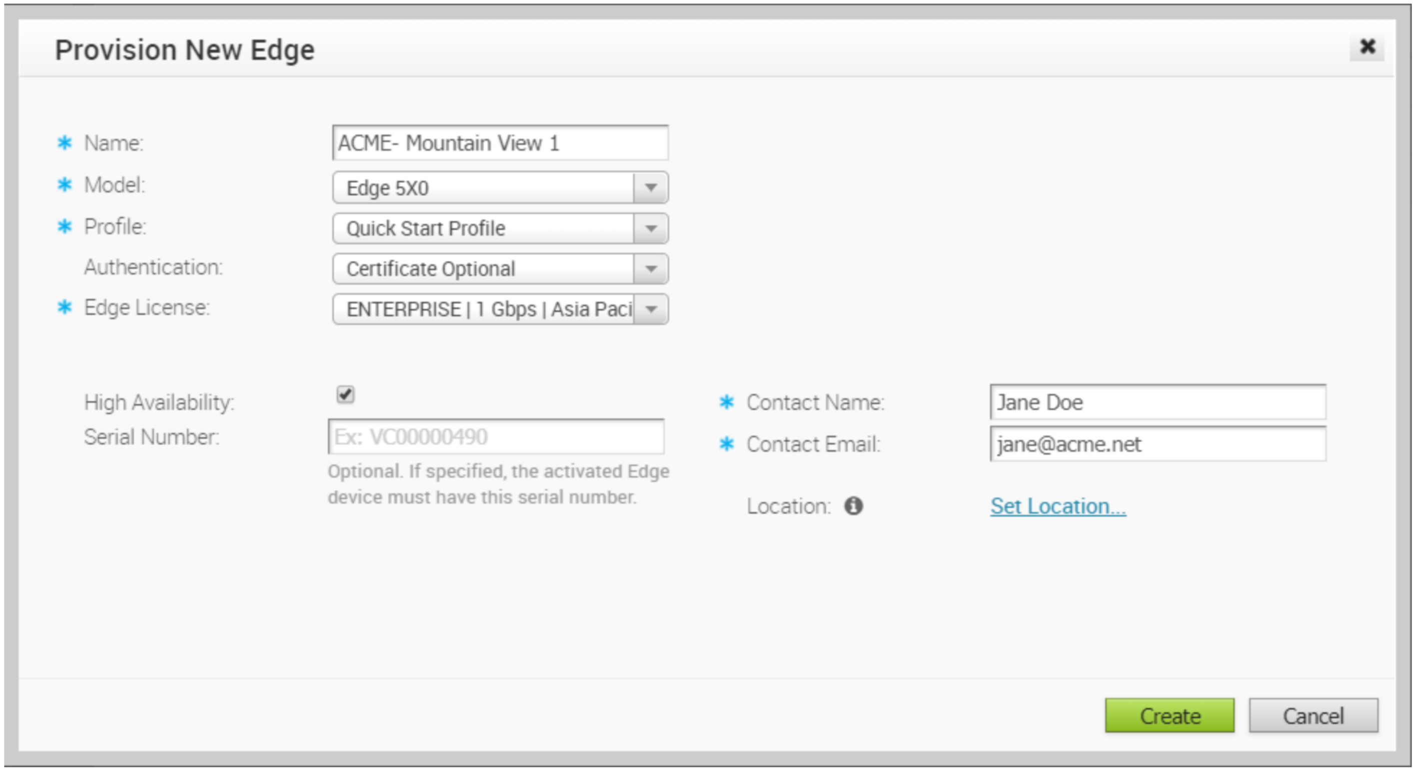
Edge	510, 510N	510-LTE	520	520V	540	610, 610C, 610N	610-LTE	620, 620C, 620N
System memory (RAM)	4 GB	4 GB	4 GB	8 GB	8 GB	4 GB	4 GB	8 GB
System flash	8 GB	8 GB	8 GB	8 GB	8 GB	16 GB	16 GB	16 GB
System storage				64 GB (SSD)				120 GB (SSD)
VNF capable (initial release)	No	No	No	Yes (3.2.0)	No	No	No	Yes (3.4.3)

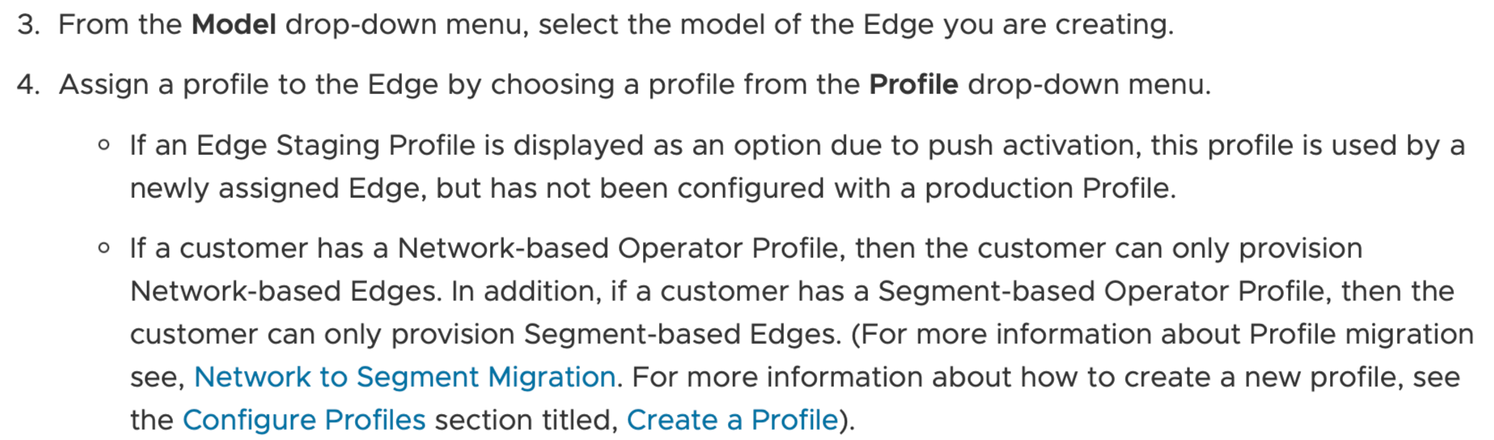
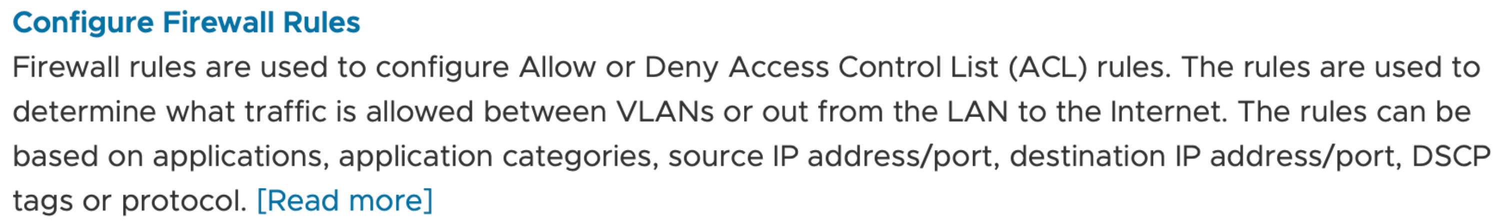
Edge	640, 640C, 640N	680, 680C, 680N	840	2000	3400, 3400C	3800, 3800C	3810
System memory (RAM)	32 GB	32 GB	32 GB	32 GB	32 GB	32 GB	32 GB
System flash	16 GB	16 GB	n/a	n/a	n/a	n/a	n/a
System storage	120 GB (SSD)	120 GB (SSD)	100 GB (SSD)	100 GB (SSD)	256 GB (SSD)	256 GB (SSD)	256 GB (SSD)
VNF capable (initial release)	Yes (3.4.3)	Yes (3.4.3)	Yes (3.2.0)	No	Yes (4.3.0)	Yes (4.3.0)	Yes (4.3.0)

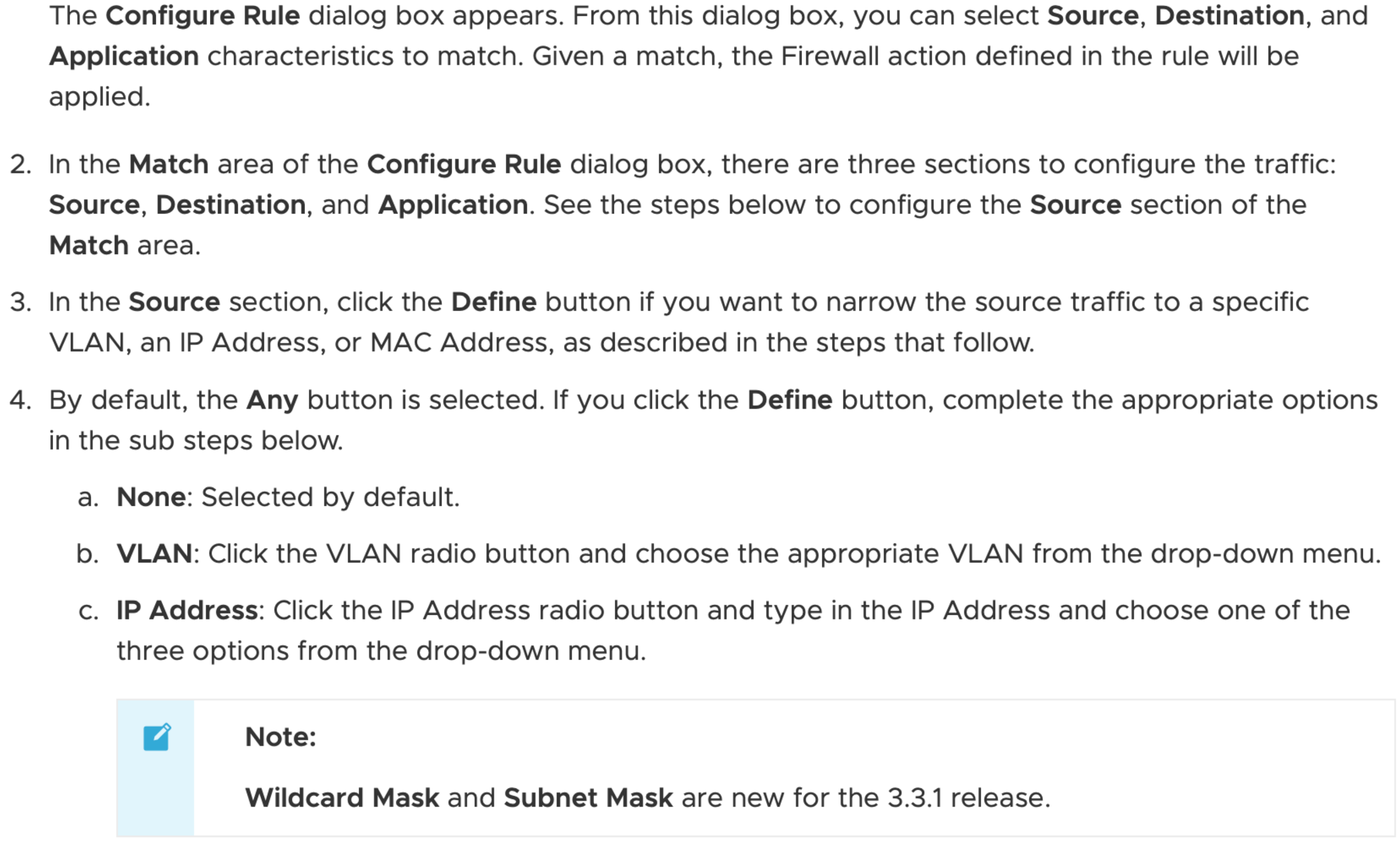
See https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-712-edge-platform-spec-ds-1020.pdf

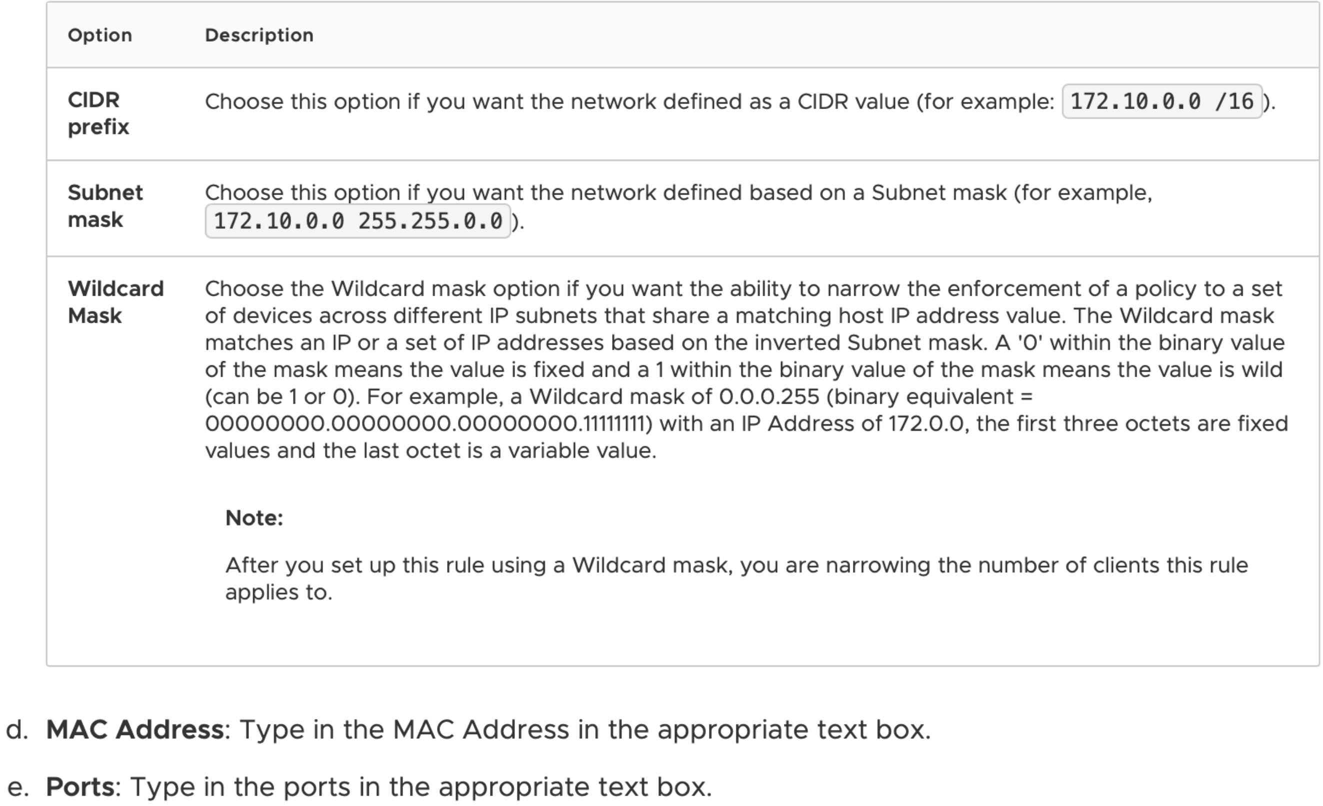
Claims	Exemplary Infringement Evidence
	 VMware SD-WAN Edge 5X0 Model Number: Edge 5X0 Part Numbers: Edge 520, Edge 540 The SD-WAN Edge 5x0 series includes the following: • 2 Gigabit Ethernet connections • LAN/WAN configurable, 2G SFP WAN connection Follow the steps below to install the Edge in the standard configuration. *See* https://sase.vmware.com/resources/edge-520  A thin "Edge" that is zero IT touch provisioned from the cloud for secured, optimized connectivity to your apps and virtualized services. The VeloCloud Edges are zero-touch, enterprise-class devices or virtual software that provide secure and optimized connectivity to private, public and hybrid applications; compute; and virtualized services. VeloCloud Edges perform deep application recognition, application and per-packet steering, on-demand remediation performance metrics and end-to-end quality of service (QoS) in addition to hosting Virtual Network Function (VNF) services. An Edge pair can be deployed to provide High Availability (HA). Edges can be deployed in branches, large sites and data centers. All other network infrastructure is provided on-demand in the cloud. The VeloCloud Orchestrator provides centralized enterprise-wide configuration and real-time monitoring, as well as orchestrates the data flow into and through the SDWAN overlay network. Additionally, it provides the one-click provisioning of virtual services across Edges, in centralized and regional enterprise service hubs and in the cloud. *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-16C592CA-8F02-4CEF-B8FB-769A0CDA0231.html

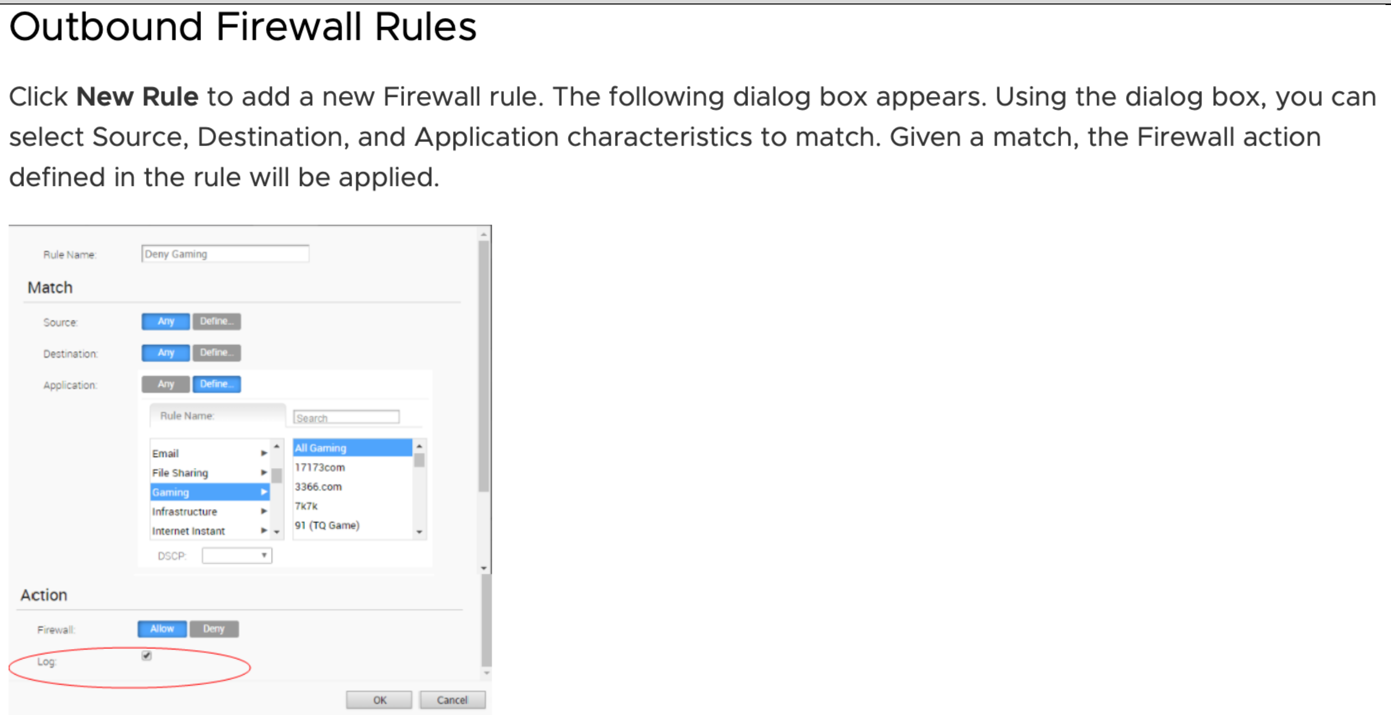
Claims	Exemplary Infringement Evidence
	 VMware SD-WAN Orchestration Office 365 skype webex Microsoft Azure servicenow salesforce Office 365 box VMware SD-WAN Gateways SaaS / IaaS VMware SD-WAN Edges Private /MPLS 3G/4G LTE SD-WAN Overlay Internet Broadband VMware SD-WAN Edges *Figure 1 VMware SD-WAN by VeloCloud* *See* VMware SD-WANTM by VeloCloud at p. 2.  Enterprise Admins can provision a single Edge or multiple Edges, such as assigning a Profile configuration to an Edge or changing other Edge specific parameters. You must create a configuration for every Edge you will deploy to a specific site. This section describes what an Enterprise Admin can provision.

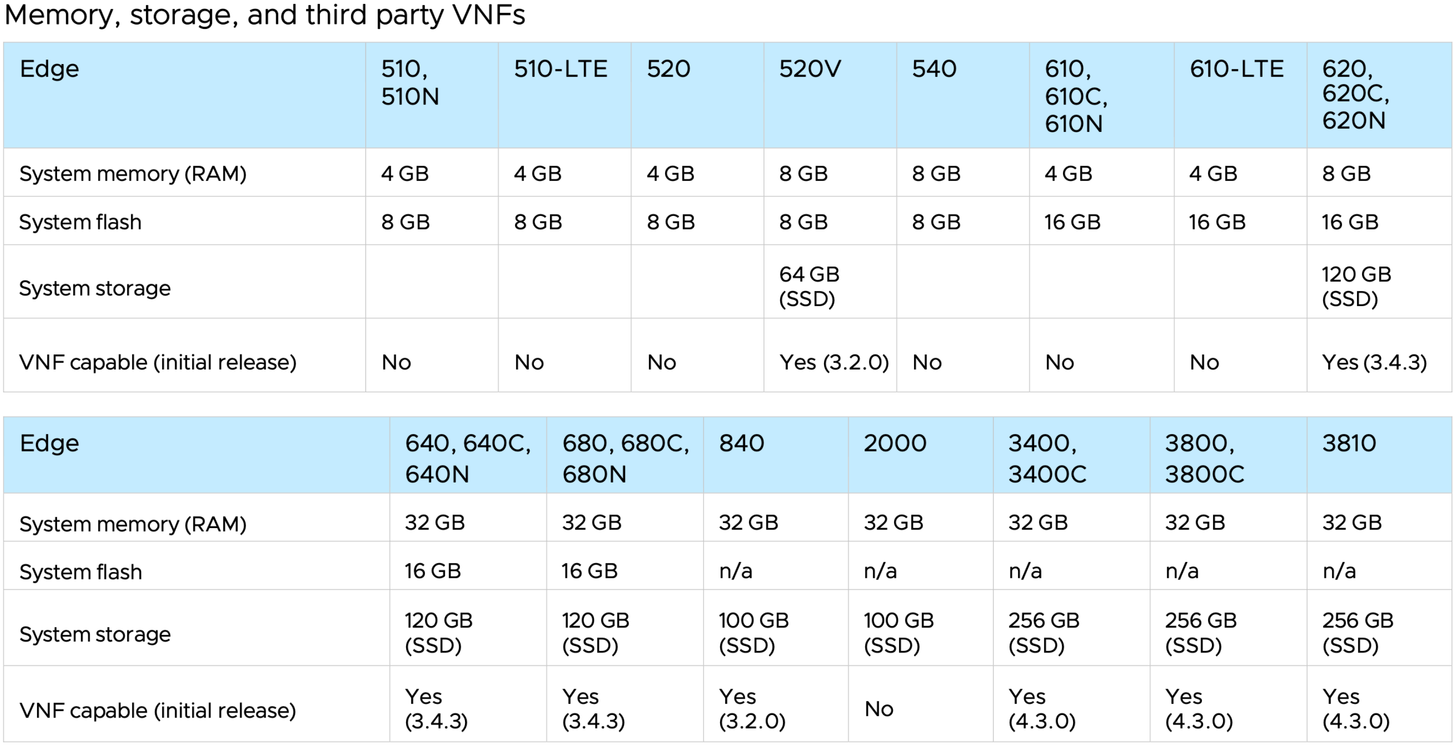
Claims	Exemplary Infringement Evidence
	See https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-0F429D7E-A399-4A57-BFE2-E592D259DBEB.html  Provision New Edge ✱ Name: ACME- Mountain View 1 ✱ Model: Edge 5X0 ✱ Profile: Quick Start Profile Authentication: Certificate Optional ✱ Edge License: ENTERPRISE | 1 Gbps | Asia Paci High Availability: ☑ Serial Number: Ex: VC00000490 Optional. If specified, the activated Edge device must have this serial number. ✱ Contact Name: Jane Doe ✱ Contact Email: jane@acme.net Location: *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-D583722C-9B15-444D-9B84-05BA0B1FDA94.html 1. In the **VeloCloud Edges** screen, click the **New Edge** button, located on the top, right corner of the VCO. 2. In the **Provision New Edge** dialog box, type a unique name for the Edge in the **Name** text field (see image below).

Claims	Exemplary Infringement Evidence
	 3. From the **Model** drop-down menu, select the model of the Edge you are creating. 4. Assign a profile to the Edge by choosing a profile from the **Profile** drop-down menu. ◦ If an Edge Staging Profile is displayed as an option due to push activation, this profile is used by a newly assigned Edge, but has not been configured with a production Profile. ◦ If a customer has a Network-based Operator Profile, then the customer can only provision Network-based Edges. In addition, if a customer has a Segment-based Operator Profile, then the customer can only provision Segment-based Edges. (For more information about Profile migration see, Network to Segment Migration. For more information about how to create a new profile, see the Configure Profiles section titled, Create a Profile). *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-D583722C-9B15-444D-9B84-05BA0B1FDA94.html  **Configure Firewall Rules** Firewall rules are used to configure Allow or Deny Access Control List (ACL) rules. The rules are used to determine what traffic is allowed between VLANs or out from the LAN to the Internet. The rules can be based on applications, application categories, source IP address/port, destination IP address/port, DSCP tags or protocol. [Read more] *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-AD64ABD4-4388-4CCD-BC16-E993C82817CC.html

Claims	Exemplary Infringement Evidence
	 The **Configure Rule** dialog box appears. From this dialog box, you can select **Source**, **Destination**, and **Application** characteristics to match. Given a match, the Firewall action defined in the rule will be applied. 2. In the **Match** area of the **Configure Rule** dialog box, there are three sections to configure the traffic: **Source**, **Destination**, and **Application**. See the steps below to configure the **Source** section of the **Match** area. 3. In the **Source** section, click the **Define** button if you want to narrow the source traffic to a specific VLAN, an IP Address, or MAC Address, as described in the steps that follow. 4. By default, the **Any** button is selected. If you click the **Define** button, complete the appropriate options in the sub steps below. a. **None**: Selected by default. b. **VLAN**: Click the VLAN radio button and choose the appropriate VLAN from the drop-down menu. c. **IP Address**: Click the IP Address radio button and type in the IP Address and choose one of the three options from the drop-down menu. **Note:** **Wildcard Mask** and **Subnet Mask** are new for the 3.3.1 release.

<table>
<tr><th>Claims</th><th>Exemplary Infringement Evidence</th></tr>
<tr><td></td><td>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>CIDR prefix</b></td><td>Choose this option if you want the network defined as a CIDR value (for example: <code>172.10.0.0 /16</code>).</td></tr>
<tr><td><b>Subnet mask</b></td><td>Choose this option if you want the network defined based on a Subnet mask (for example, <code>172.10.0.0 255.255.0.0</code>).</td></tr>
<tr><td><b>Wildcard Mask</b></td><td>Choose the Wildcard mask option if you want the ability to narrow the enforcement of a policy to a set of devices across different IP subnets that share a matching host IP address value. The Wildcard mask matches an IP or a set of IP addresses based on the inverted Subnet mask. A '0' within the binary value of the mask means the value is fixed and a 1 within the binary value of the mask means the value is wild (can be 1 or 0). For example, a Wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111) with an IP Address of 172.0.0, the first three octets are fixed values and the last octet is a variable value.
<b>Note:</b>
After you set up this rule using a Wildcard mask, you are narrowing the number of clients this rule applies to.</td></tr>
</table>
d. <b>MAC Address</b>: Type in the MAC Address in the appropriate text box.
e. <b>Ports</b>: Type in the ports in the appropriate text box.
<i>See</i> https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-2CA50320-D08E-493E-B7EA-5DBAB441BAD4.html
</td></tr>
</table>

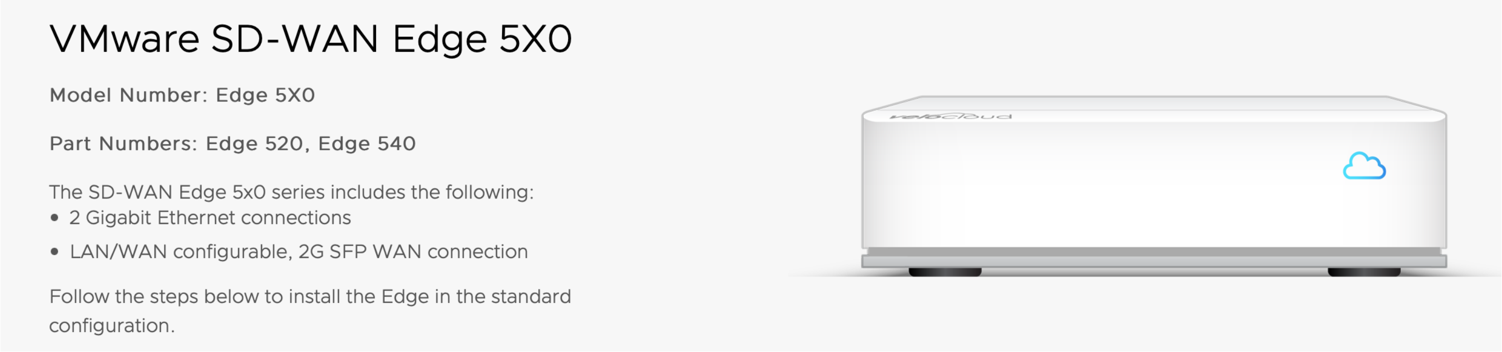
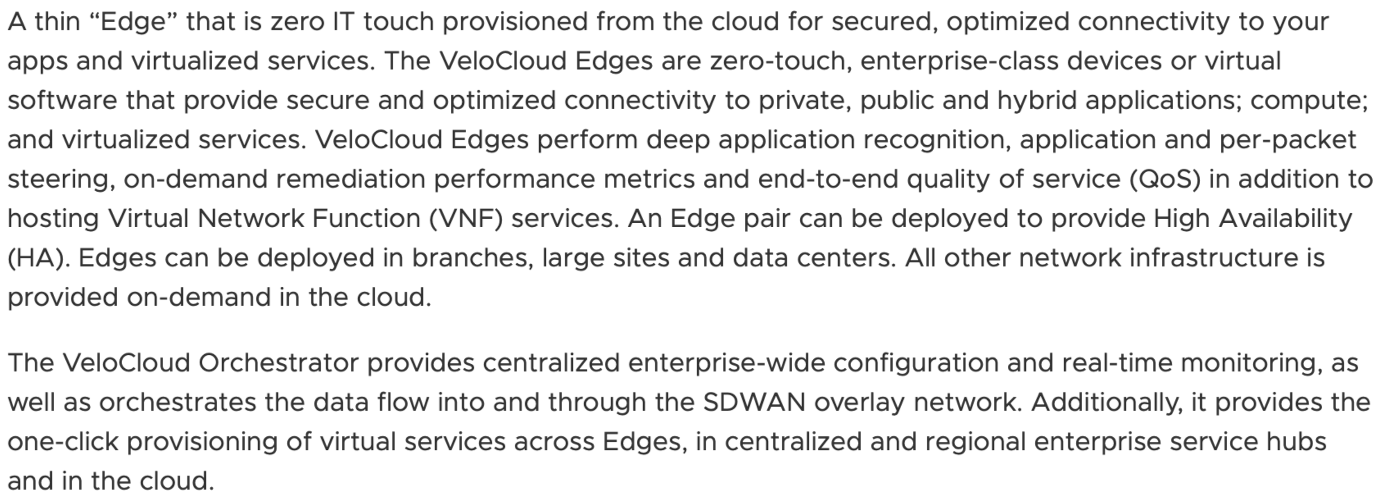
Claims	Exemplary Infringement Evidence
	 **Outbound Firewall Rules** Click **New Rule** to add a new Firewall rule. The following dialog box appears. Using the dialog box, you can select Source, Destination, and Application characteristics to match. Given a match, the Firewall action defined in the rule will be applied. Rule Name: Deny Gaming Match Source: Any Define... Destination: Any Define... Application: Any Define... Rule Name: Search Email ▸ File Sharing ▸ Gaming ▸ Infrastructure ▸ Internet Instant ▸ All Gaming 17173com 3366.com 7k7k 91 (TQ Game) DSCP: Action Firewall: Allow Deny Log: ☑ OK Cancel *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-2CA50320-D08E-493E-B7EA-5DBAB441BAD4.html
[15b] a memory circuit coupled to the forwarding circuit, the memory circuit operable to store packets and operable to	Each Accused Product comprises a memory circuit coupled to the forwarding circuit, the memory circuit operable to store packets and operable to store an enhanced access control list and a dynamic access control list.

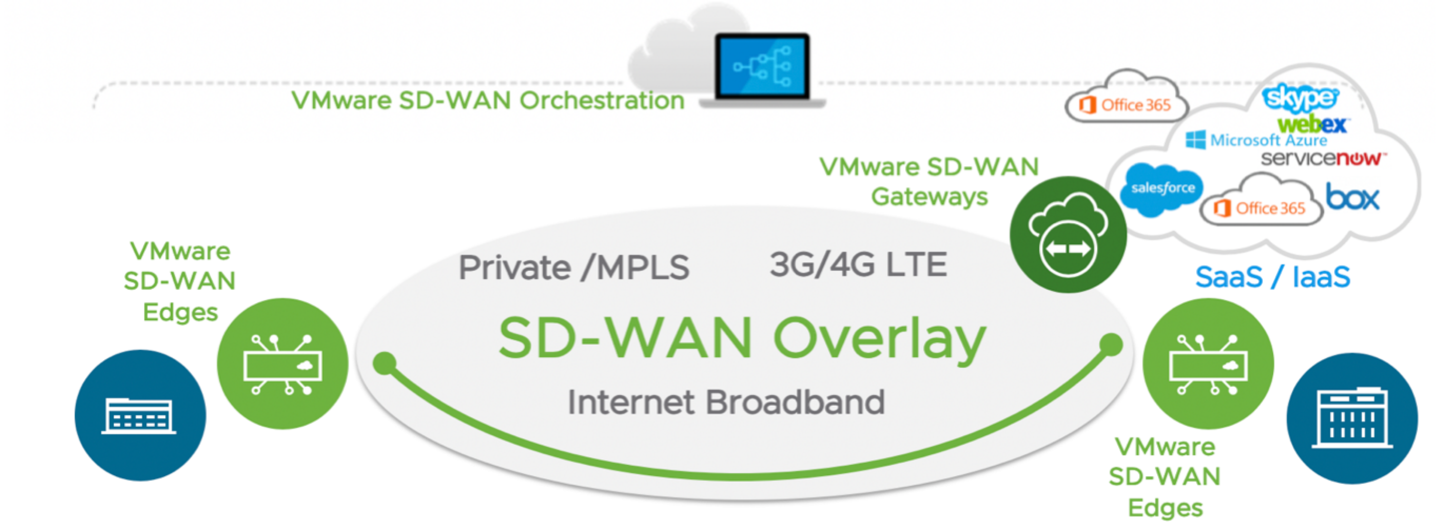
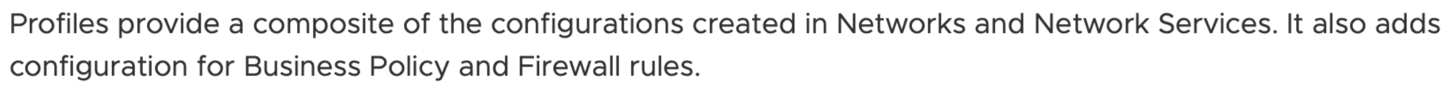
Claims	Exemplary Infringement Evidence
store an enhanced access control list and a dynamic access control list; and	 *See* https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-712-edge-platform-spec-ds-1020.pdf

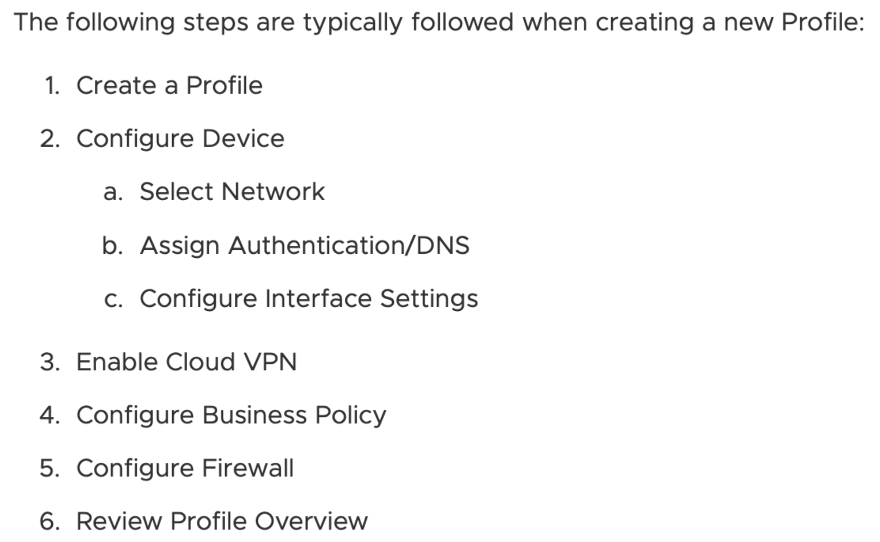
Memory, storage, and third party VNFs

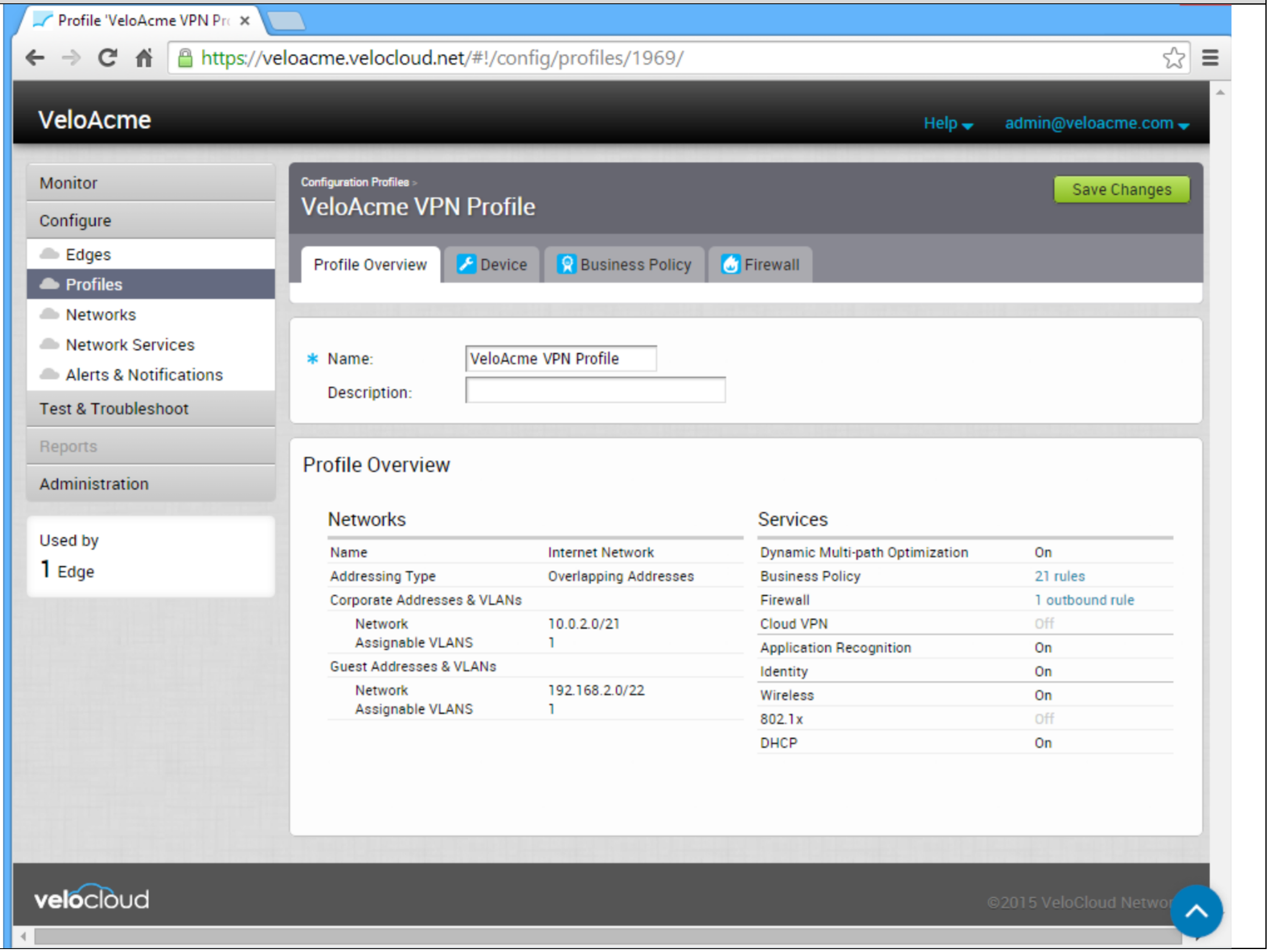
Edge	510, 510N	510-LTE	520	520V	540	610, 610C, 610N	610-LTE	620, 620C, 620N
System memory (RAM)	4 GB	4 GB	4 GB	8 GB	8 GB	4 GB	4 GB	8 GB
System flash	8 GB	8 GB	8 GB	8 GB	8 GB	16 GB	16 GB	16 GB
System storage				64 GB (SSD)				120 GB (SSD)
VNF capable (initial release)	No	No	No	Yes (3.2.0)	No	No	No	Yes (3.4.3)

Edge	640, 640C, 640N	680, 680C, 680N	840	2000	3400, 3400C	3800, 3800C	3810
System memory (RAM)	32 GB	32 GB	32 GB	32 GB	32 GB	32 GB	32 GB
System flash	16 GB	16 GB	n/a	n/a	n/a	n/a	n/a
System storage	120 GB (SSD)	120 GB (SSD)	100 GB (SSD)	100 GB (SSD)	256 GB (SSD)	256 GB (SSD)	256 GB (SSD)
VNF capable (initial release)	Yes (3.4.3)	Yes (3.4.3)	Yes (3.2.0)	No	Yes (4.3.0)	Yes (4.3.0)	Yes (4.3.0)

Claims	Exemplary Infringement Evidence
	 VMware SD-WAN Edge 5X0 Model Number: Edge 5X0 Part Numbers: Edge 520, Edge 540 The SD-WAN Edge 5x0 series includes the following: • 2 Gigabit Ethernet connections • LAN/WAN configurable, 2G SFP WAN connection Follow the steps below to install the Edge in the standard configuration. *See* https://sase.vmware.com/resources/edge-520  A thin "Edge" that is zero IT touch provisioned from the cloud for secured, optimized connectivity to your apps and virtualized services. The VeloCloud Edges are zero-touch, enterprise-class devices or virtual software that provide secure and optimized connectivity to private, public and hybrid applications; compute; and virtualized services. VeloCloud Edges perform deep application recognition, application and per-packet steering, on-demand remediation performance metrics and end-to-end quality of service (QoS) in addition to hosting Virtual Network Function (VNF) services. An Edge pair can be deployed to provide High Availability (HA). Edges can be deployed in branches, large sites and data centers. All other network infrastructure is provided on-demand in the cloud. The VeloCloud Orchestrator provides centralized enterprise-wide configuration and real-time monitoring, as well as orchestrates the data flow into and through the SDWAN overlay network. Additionally, it provides the one-click provisioning of virtual services across Edges, in centralized and regional enterprise service hubs and in the cloud. *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-16C592CA-8F02-4CEF-B8FB-769A0CDA0231.html

Claims	Exemplary Infringement Evidence
	 VMware SD-WAN Orchestration Office 365 skype webex Microsoft Azure servicenow salesforce Office 365 box VMware SD-WAN Gateways SaaS / IaaS VMware SD-WAN Edges Private /MPLS 3G/4G LTE SD-WAN Overlay Internet Broadband VMware SD-WAN Edges *Figure 1 VMware SD-WAN by VeloCloud* *See* VMware SD-WANTM by VeloCloud at p. 2.  Profiles provide a composite of the configurations created in Networks and Network Services. It also adds configuration for Business Policy and Firewall rules.

Claims	Exemplary Infringement Evidence
	See https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-D174B662-089C-4EC9-A389-682363C40ADF.html  The following steps are typically followed when creating a new Profile: 1. Create a Profile 2. Configure Device a. Select Network b. Assign Authentication/DNS c. Configure Interface Settings 3. Enable Cloud VPN 4. Configure Business Policy 5. Configure Firewall 6. Review Profile Overview *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-8C960BF4-AE88-4C9D-9750-FA96FBA1C0F3.html

Claims	Exemplary Infringement Evidence
	

https://veloacme.velocloud.net/#!/config/profiles/1969/

Used by
1 Edge

VeloAcme VPN Profile

* Name: VeloAcme VPN Profile

Description:

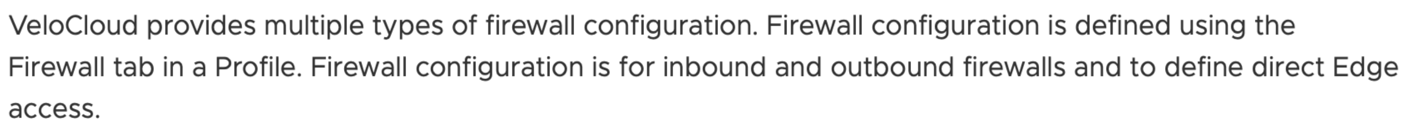
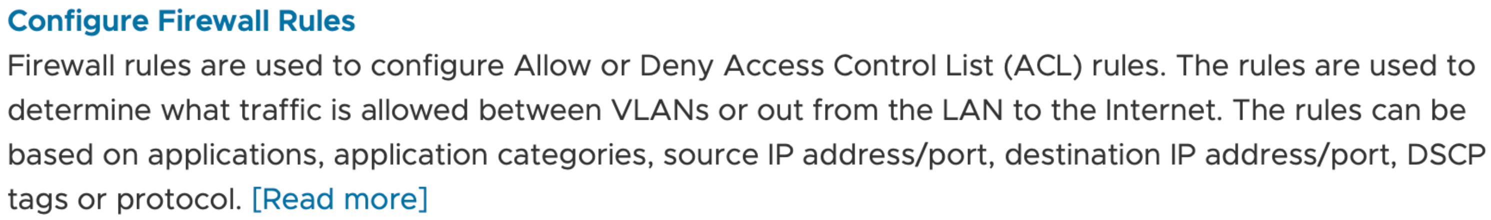
Profile Overview

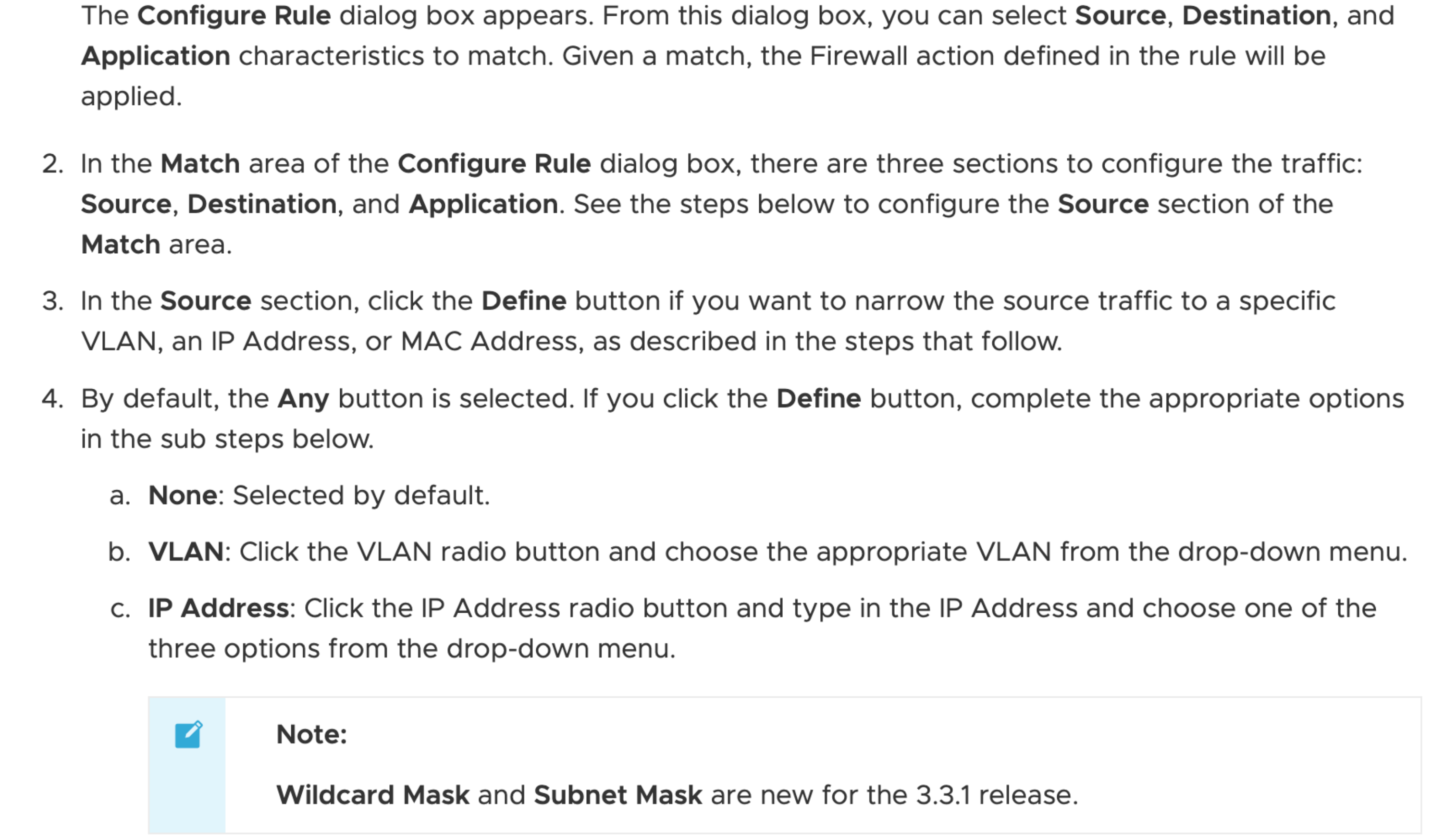
Networks

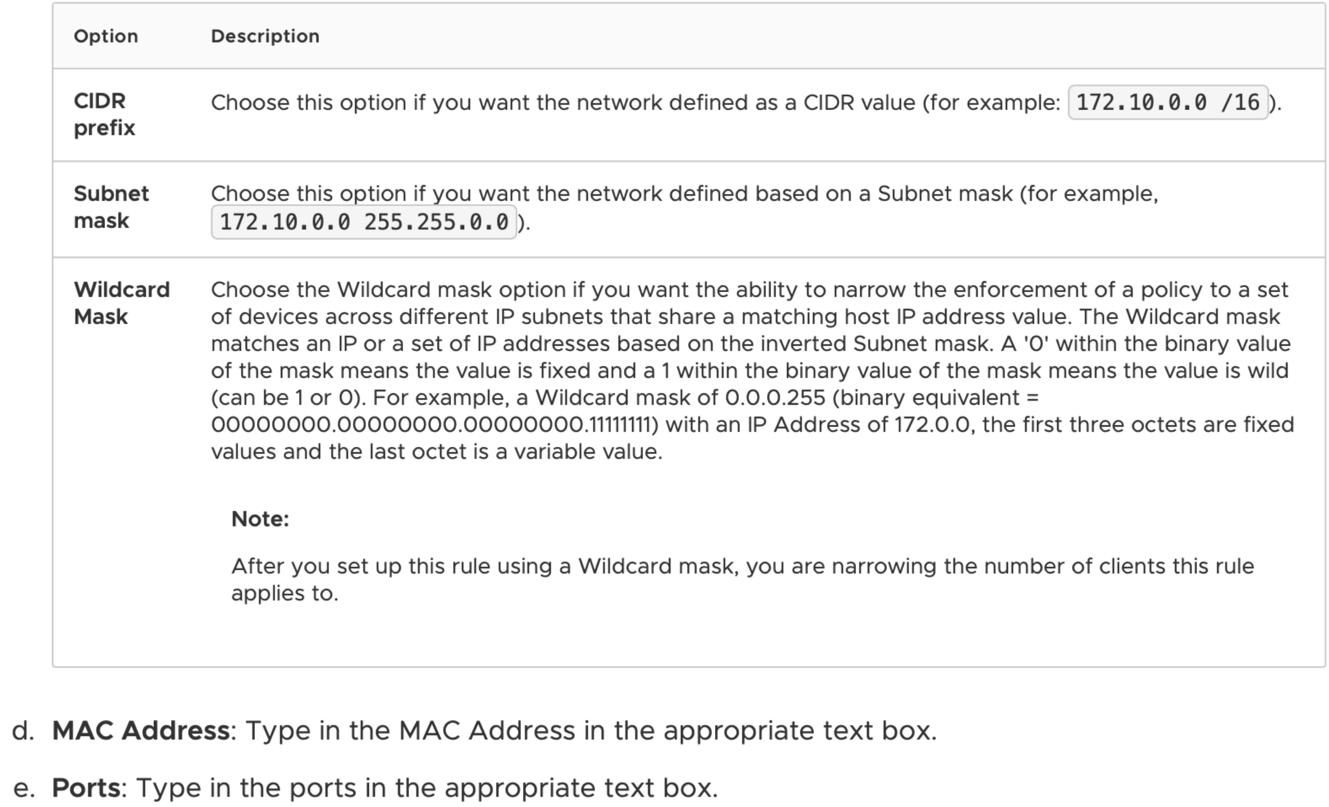
Name	Internet Network
Addressing Type	Overlapping Addresses
Corporate Addresses & VLANs	
Network Assignable VLANS	10.0.2.0/21 1
Guest Addresses & VLANs	
Network Assignable VLANS	192.168.2.0/22 1

Services

Dynamic Multi-path Optimization	On
Business Policy	21 rules
Firewall	1 outbound rule
Cloud VPN	Off
Application Recognition	On
Identity	On
Wireless	On
802.1x	Off
DHCP	On

Claims	Exemplary Infringement Evidence
	See https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-8C960BF4-AE88-4C9D-9750-FA96FBA1C0F3.html  VeloCloud provides multiple types of firewall configuration. Firewall configuration is defined using the Firewall tab in a Profile. Firewall configuration is for inbound and outbound firewalls and to define direct Edge access. *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-AD64ABD4-4388-4CCD-BC16-E993C82817CC.html  **Configure Firewall Rules** Firewall rules are used to configure Allow or Deny Access Control List (ACL) rules. The rules are used to determine what traffic is allowed between VLANs or out from the LAN to the Internet. The rules can be based on applications, application categories, source IP address/port, destination IP address/port, DSCP tags or protocol. [Read more] *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-AD64ABD4-4388-4CCD-BC16-E993C82817CC.html

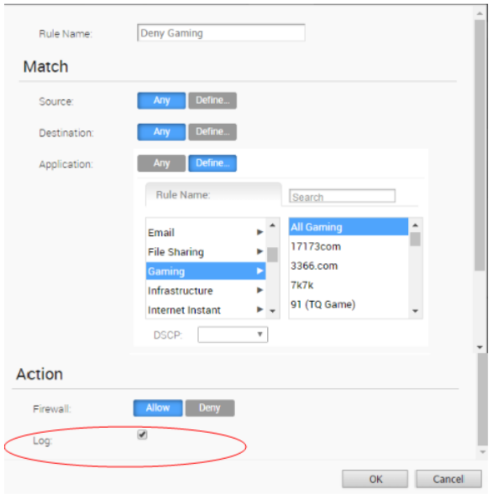
Claims	Exemplary Infringement Evidence
	 The **Configure Rule** dialog box appears. From this dialog box, you can select **Source**, **Destination**, and **Application** characteristics to match. Given a match, the Firewall action defined in the rule will be applied. 2. In the **Match** area of the **Configure Rule** dialog box, there are three sections to configure the traffic: **Source**, **Destination**, and **Application**. See the steps below to configure the **Source** section of the **Match** area. 3. In the **Source** section, click the **Define** button if you want to narrow the source traffic to a specific VLAN, an IP Address, or MAC Address, as described in the steps that follow. 4. By default, the **Any** button is selected. If you click the **Define** button, complete the appropriate options in the sub steps below. a. **None**: Selected by default. b. **VLAN**: Click the VLAN radio button and choose the appropriate VLAN from the drop-down menu. c. **IP Address**: Click the IP Address radio button and type in the IP Address and choose one of the three options from the drop-down menu. **Note:** **Wildcard Mask** and **Subnet Mask** are new for the 3.3.1 release.

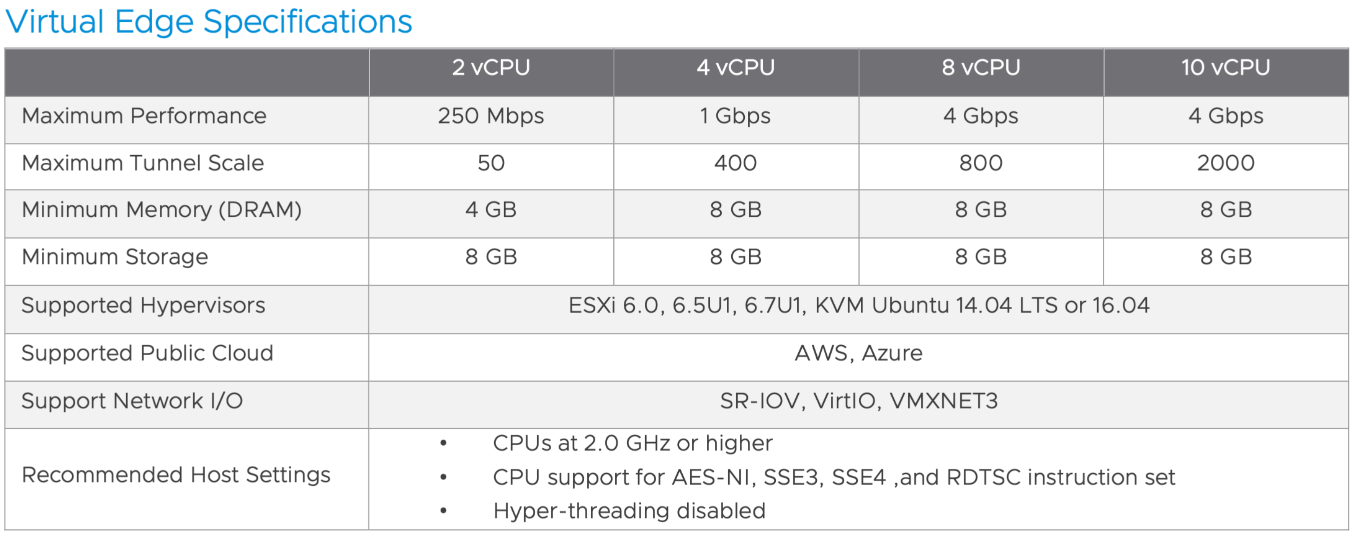
<table>
<tr><th>Claims</th><th>Exemplary Infringement Evidence</th></tr>
<tr><td></td><td>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>CIDR prefix</b></td><td>Choose this option if you want the network defined as a CIDR value (for example: <code>172.10.0.0 /16</code>).</td></tr>
<tr><td><b>Subnet mask</b></td><td>Choose this option if you want the network defined based on a Subnet mask (for example, <code>172.10.0.0 255.255.0.0</code>).</td></tr>
<tr><td><b>Wildcard Mask</b></td><td>Choose the Wildcard mask option if you want the ability to narrow the enforcement of a policy to a set of devices across different IP subnets that share a matching host IP address value. The Wildcard mask matches an IP or a set of IP addresses based on the inverted Subnet mask. A '0' within the binary value of the mask means the value is fixed and a 1 within the binary value of the mask means the value is wild (can be 1 or 0). For example, a Wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111) with an IP Address of 172.0.0, the first three octets are fixed values and the last octet is a variable value.

<b>Note:</b>

After you set up this rule using a Wildcard mask, you are narrowing the number of clients this rule applies to.</td></tr>
</table>

d. <b>MAC Address</b>: Type in the MAC Address in the appropriate text box.
e. <b>Ports</b>: Type in the ports in the appropriate text box.
<i>See</i> https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-2CA50320-D08E-493E-B7EA-5DBAB441BAD4.html
</td></tr>
</table>

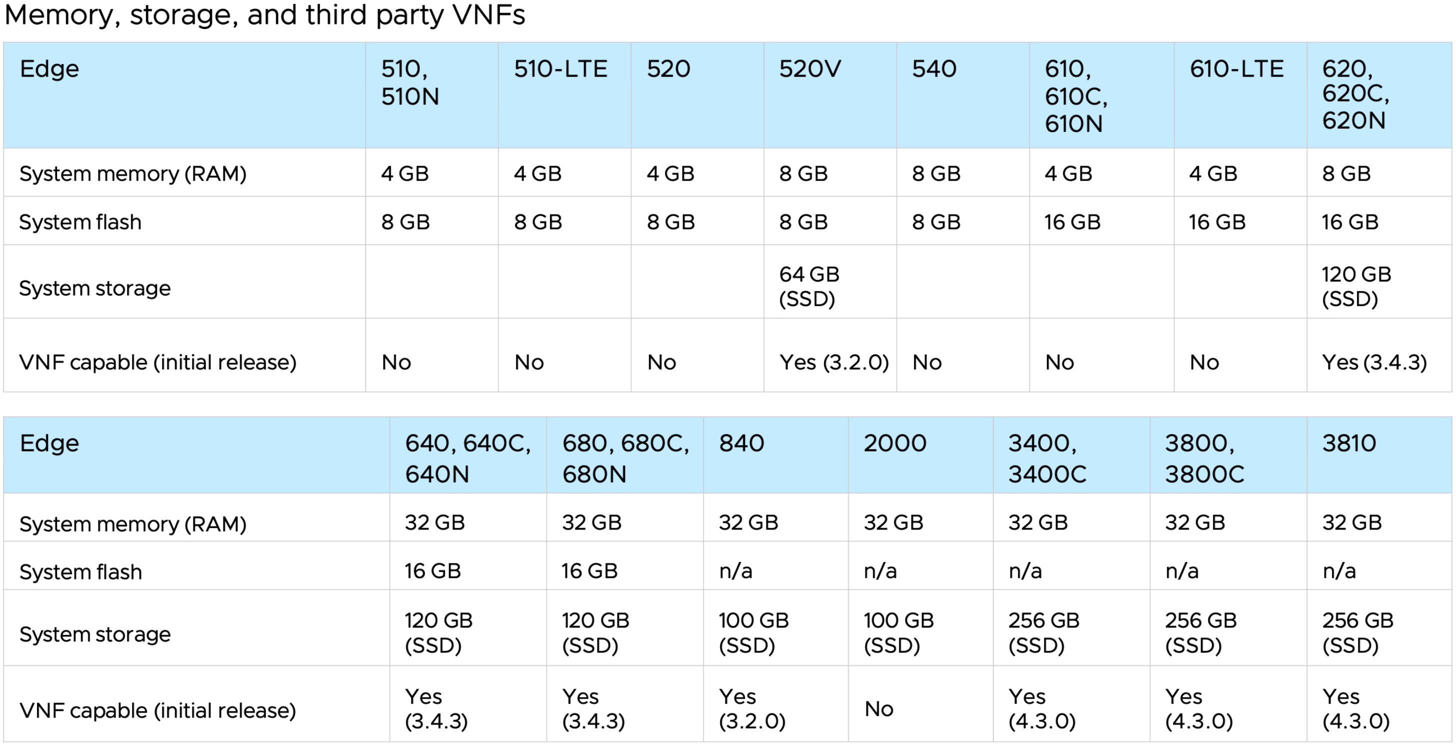
Claims	Exemplary Infringement Evidence
	Outbound Firewall Rules Click **New Rule** to add a new Firewall rule. The following dialog box appears. Using the dialog box, you can select Source, Destination, and Application characteristics to match. Given a match, the Firewall action defined in the rule will be applied. Rule Name: Deny Gaming Match Source: Any Define... Destination: Any Define... Application: Any Define... Rule Name: Search Email ▸ File Sharing ▸ Gaming ▸ Infrastructure ▸ Internet Instant ▸ All Gaming 17173com 3366.com 7k7k 91 (TQ Game) DSCP: Action Firewall: Allow Deny Log: ☑ OK Cancel *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-2CA50320-D08E-493E-B7EA-5DBAB441BAD4.html
[15c] a processor coupled to the forwarding circuit and to the memory circuit, the processor operable to	Each Accused Product comprises a processor coupled to the forwarding circuit and to the memory circuit, the processor operable to define the specific packets detected by the forwarding circuit and operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and store the dynamic access control list in the memory circuit, and further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets.

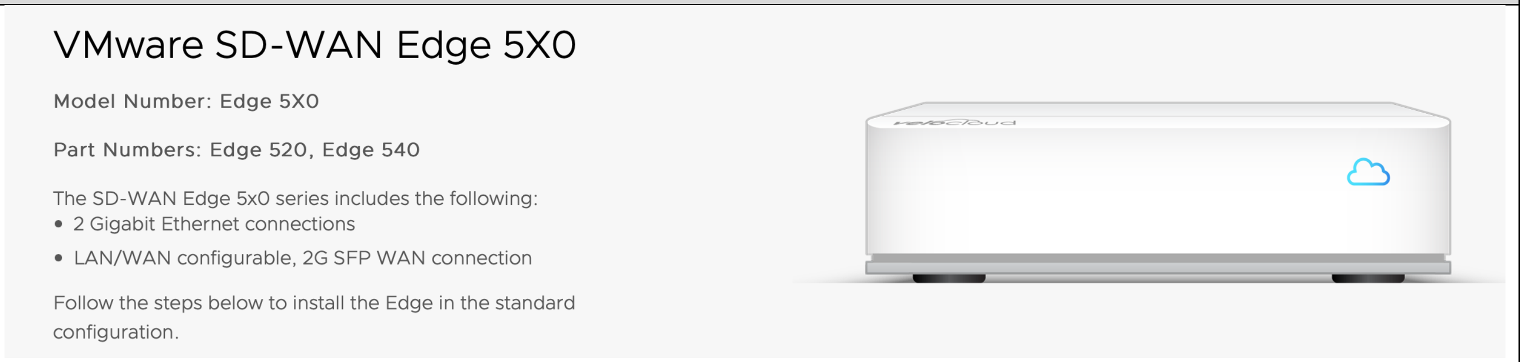
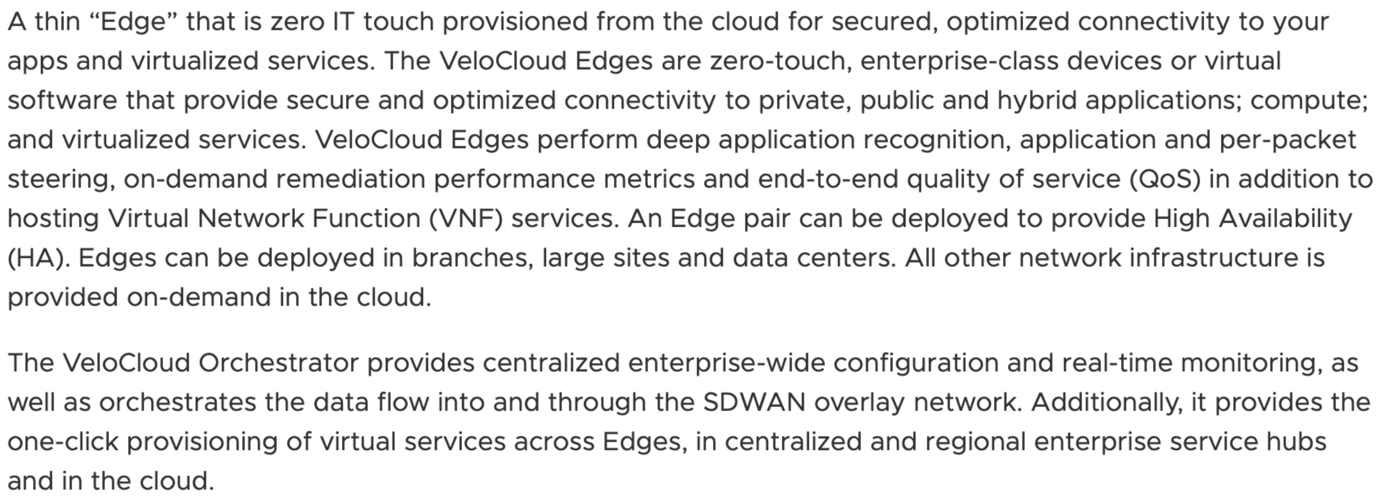
<table>
<tr><th>Claims</th><th>Exemplary Infringement Evidence</th></tr>
<tr><td>define the specific packets detected by the forwarding circuit and operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and store the dynamic access control list in the memory circuit, and further operable to provide the specific packets to the processor port of the forwarding</td><td>


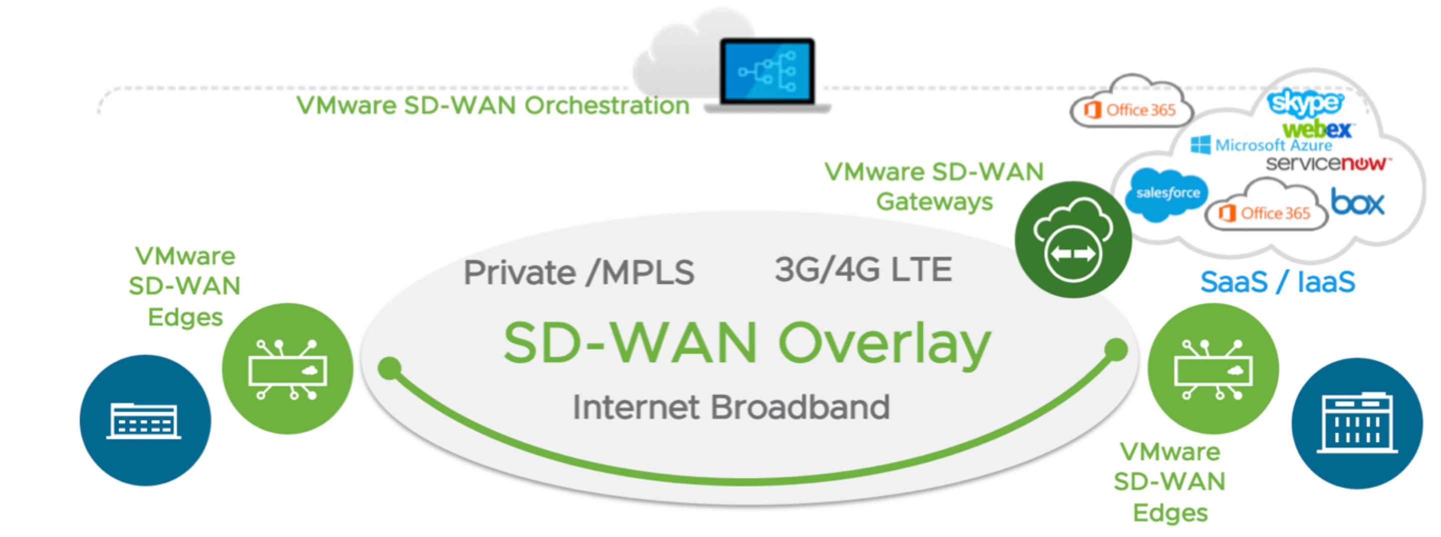
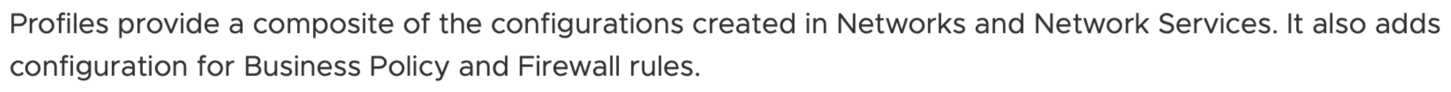
Virtual Edge Specifications

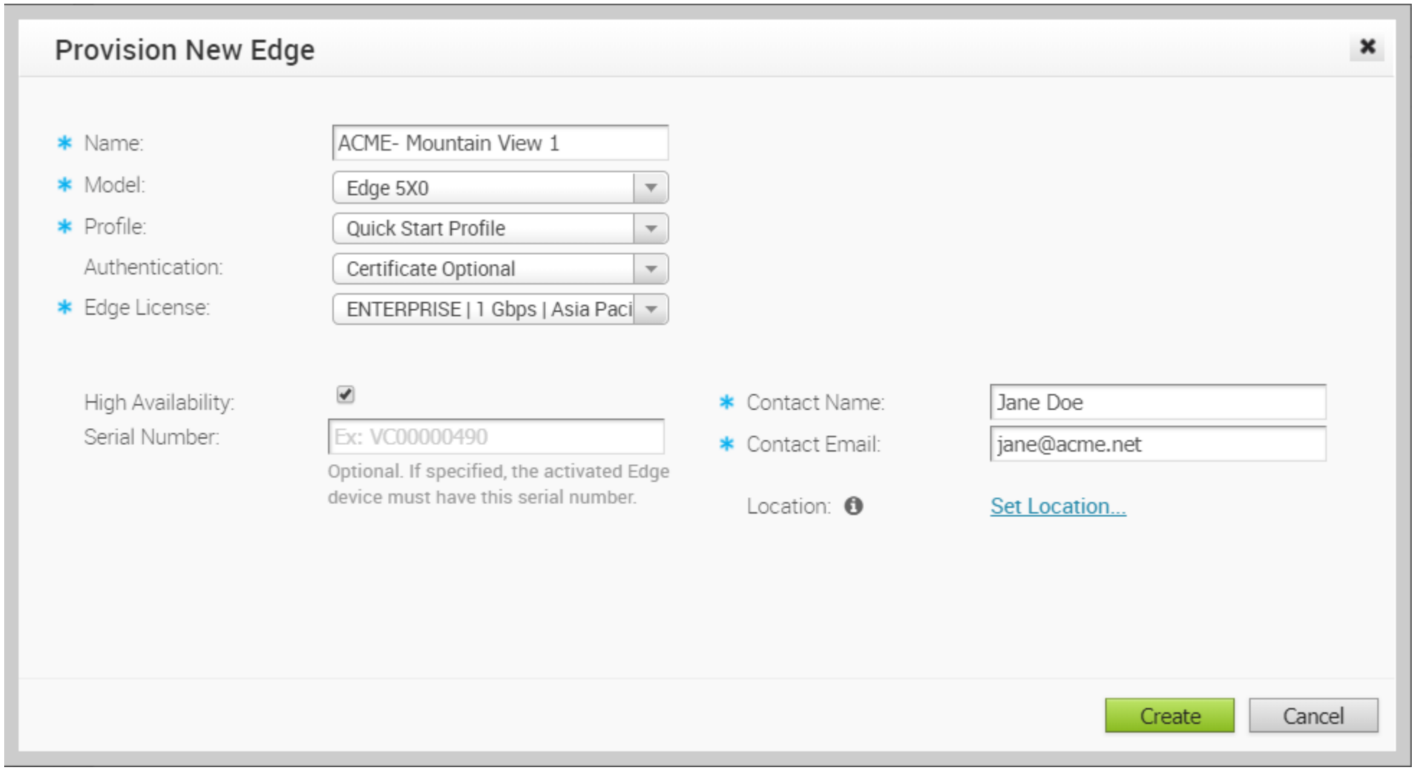
<table>
<tr><th></th><th>2 vCPU</th><th>4 vCPU</th><th>8 vCPU</th><th>10 vCPU</th></tr>
<tr><td>Maximum Performance</td><td>250 Mbps</td><td>1 Gbps</td><td>4 Gbps</td><td>4 Gbps</td></tr>
<tr><td>Maximum Tunnel Scale</td><td>50</td><td>400</td><td>800</td><td>2000</td></tr>
<tr><td>Minimum Memory (DRAM)</td><td>4 GB</td><td>8 GB</td><td>8 GB</td><td>8 GB</td></tr>
<tr><td>Minimum Storage</td><td>8 GB</td><td>8 GB</td><td>8 GB</td><td>8 GB</td></tr>
<tr><td>Supported Hypervisors</td><td colspan="4">ESXi 6.0, 6.5U1, 6.7U1, KVM Ubuntu 14.04 LTS or 16.04</td></tr>
<tr><td>Supported Public Cloud</td><td colspan="4">AWS, Azure</td></tr>
<tr><td>Support Network I/O</td><td colspan="4">SR-IOV, VirtIO, VMXNET3</td></tr>
<tr><td>Recommended Host Settings</td><td colspan="4">• CPUs at 2.0 GHz or higher
• CPU support for AES-NI, SSE3, SSE4 ,and RDTSC instruction set
• Hyper-threading disabled</td></tr>
</table>

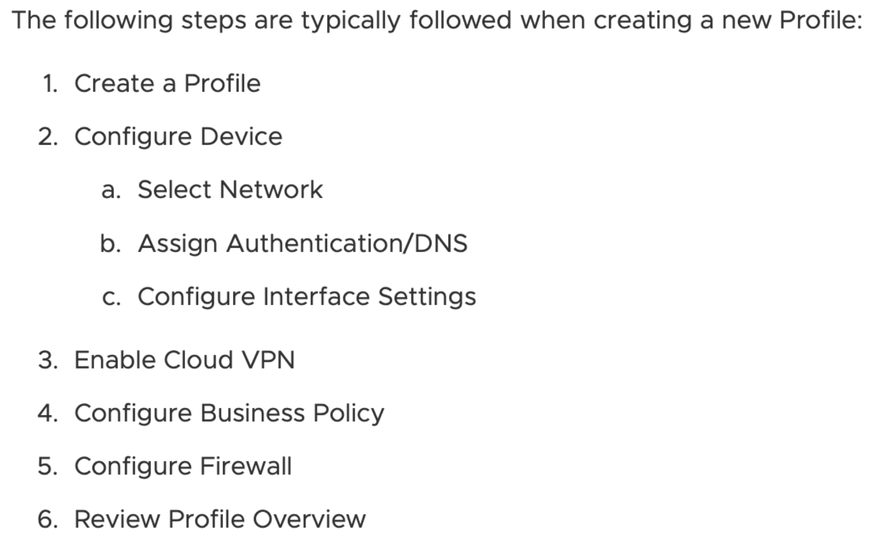
See VMware SD-WANTM by VeloCloud at p. 7.
</td></tr>
</table>

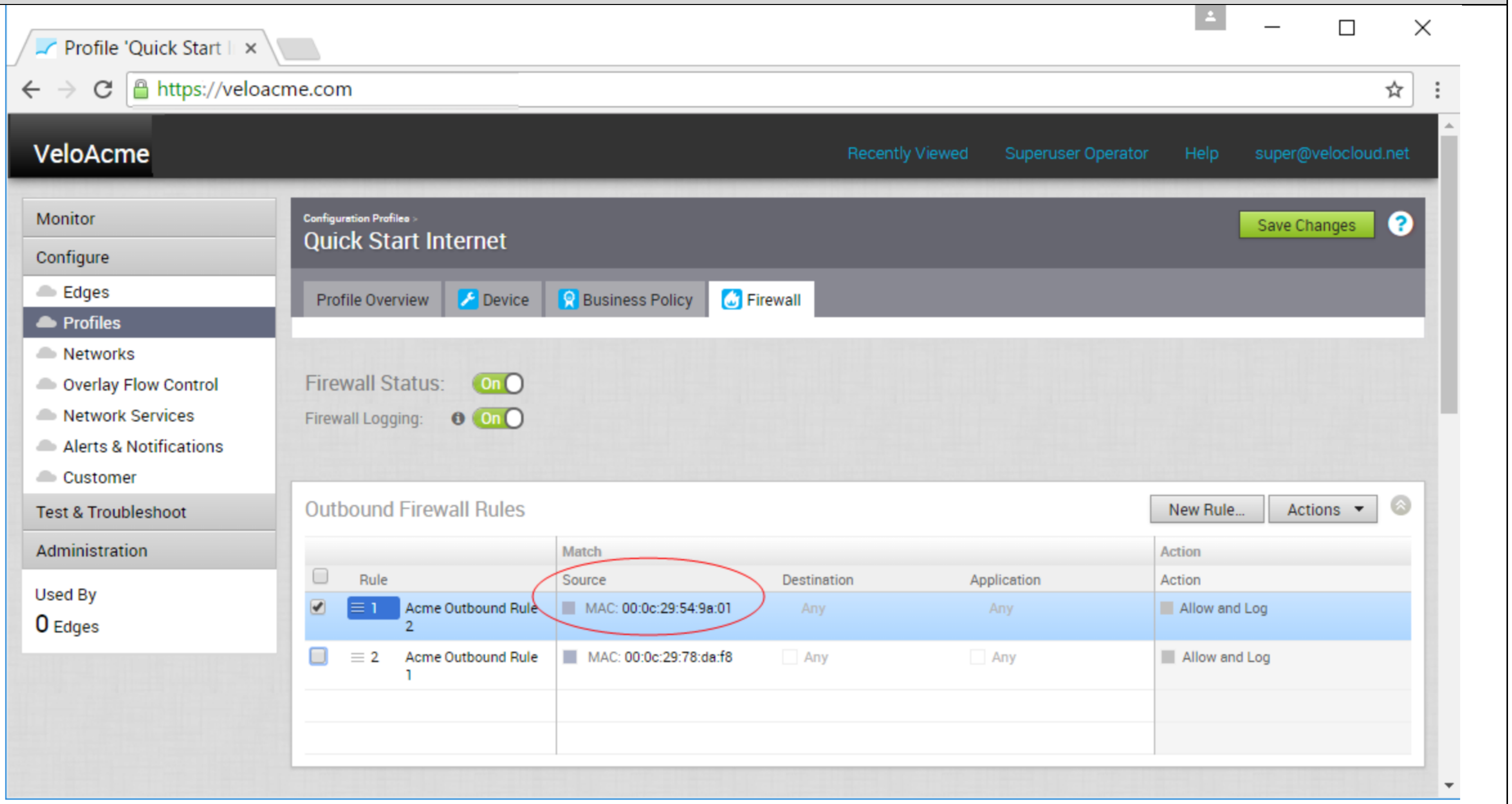
<table>
<tr><th>Claims</th><th>Exemplary Infringement Evidence</th></tr>
<tr><td>circuit after processing the packets.</td><td>

Memory, storage, and third party VNFs
<table>
<tr><th>Edge</th><th>510, 510N</th><th>510-LTE</th><th>520</th><th>520V</th><th>540</th><th>610, 610C, 610N</th><th>610-LTE</th><th>620, 620C, 620N</th></tr>
<tr><td>System memory (RAM)</td><td>4 GB</td><td>4 GB</td><td>4 GB</td><td>8 GB</td><td>8 GB</td><td>4 GB</td><td>4 GB</td><td>8 GB</td></tr>
<tr><td>System flash</td><td>8 GB</td><td>8 GB</td><td>8 GB</td><td>8 GB</td><td>8 GB</td><td>16 GB</td><td>16 GB</td><td>16 GB</td></tr>
<tr><td>System storage</td><td></td><td></td><td></td><td>64 GB (SSD)</td><td></td><td></td><td></td><td>120 GB (SSD)</td></tr>
<tr><td>VNF capable (initial release)</td><td>No</td><td>No</td><td>No</td><td>Yes (3.2.0)</td><td>No</td><td>No</td><td>No</td><td>Yes (3.4.3)</td></tr>
</table>
<table>
<tr><th>Edge</th><th>640, 640C, 640N</th><th>680, 680C, 680N</th><th>840</th><th>2000</th><th>3400, 3400C</th><th>3800, 3800C</th><th>3810</th></tr>
<tr><td>System memory (RAM)</td><td>32 GB</td><td>32 GB</td><td>32 GB</td><td>32 GB</td><td>32 GB</td><td>32 GB</td><td>32 GB</td></tr>
<tr><td>System flash</td><td>16 GB</td><td>16 GB</td><td>n/a</td><td>n/a</td><td>n/a</td><td>n/a</td><td>n/a</td></tr>
<tr><td>System storage</td><td>120 GB (SSD)</td><td>120 GB (SSD)</td><td>100 GB (SSD)</td><td>100 GB (SSD)</td><td>256 GB (SSD)</td><td>256 GB (SSD)</td><td>256 GB (SSD)</td></tr>
<tr><td>VNF capable (initial release)</td><td>Yes (3.4.3)</td><td>Yes (3.4.3)</td><td>Yes (3.2.0)</td><td>No</td><td>Yes (4.3.0)</td><td>Yes (4.3.0)</td><td>Yes (4.3.0)</td></tr>
</table>
See https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-712-edge-platform-spec-ds-1020.pdf
</td></tr>
</table>

Claims	Exemplary Infringement Evidence
	 VMware SD-WAN Edge 5X0 Model Number: Edge 5X0 Part Numbers: Edge 520, Edge 540 The SD-WAN Edge 5x0 series includes the following: • 2 Gigabit Ethernet connections • LAN/WAN configurable, 2G SFP WAN connection Follow the steps below to install the Edge in the standard configuration. *See* https://sase.vmware.com/resources/edge-520  A thin “Edge” that is zero IT touch provisioned from the cloud for secured, optimized connectivity to your apps and virtualized services. The VeloCloud Edges are zero-touch, enterprise-class devices or virtual software that provide secure and optimized connectivity to private, public and hybrid applications; compute; and virtualized services. VeloCloud Edges perform deep application recognition, application and per-packet steering, on-demand remediation performance metrics and end-to-end quality of service (QoS) in addition to hosting Virtual Network Function (VNF) services. An Edge pair can be deployed to provide High Availability (HA). Edges can be deployed in branches, large sites and data centers. All other network infrastructure is provided on-demand in the cloud. The VeloCloud Orchestrator provides centralized enterprise-wide configuration and real-time monitoring, as well as orchestrates the data flow into and through the SDWAN overlay network. Additionally, it provides the one-click provisioning of virtual services across Edges, in centralized and regional enterprise service hubs and in the cloud. *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-16C592CA-8F02-4CEF-B8FB-769A0CDA0231.html

Claims	Exemplary Infringement Evidence
	 VMware SD-WAN Orchestration VMware SD-WAN Gateways VMware SD-WAN Edges Private /MPLS 3G/4G LTE SD-WAN Overlay Internet Broadband SaaS / IaaS Office 365 skype webex Microsoft Azure servicenow salesforce box VMware SD-WAN Edges *Figure 1 VMware SD-WAN by VeloCloud* *See* VMware SD-WANTM by VeloCloud at p. 2.  Profiles provide a composite of the configurations created in Networks and Network Services. It also adds configuration for Business Policy and Firewall rules.

Claims	Exemplary Infringement Evidence
	See https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-D174B662-089C-4EC9-A389-682363C40ADF.html  Provision New Edge * Name: ACME- Mountain View 1 * Model: Edge 5X0 * Profile: Quick Start Profile Authentication: Certificate Optional * Edge License: ENTERPRISE | 1 Gbps | Asia Paci High Availability: ☑ Serial Number: Ex: VC00000490 Optional. If specified, the activated Edge device must have this serial number. * Contact Name: Jane Doe * Contact Email: jane@acme.net Location: Set Location... *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-D583722C-9B15-444D-9B84-05BA0B1FDA94.html

Claims	Exemplary Infringement Evidence
	 The following steps are typically followed when creating a new Profile: 1. Create a Profile 2. Configure Device a. Select Network b. Assign Authentication/DNS c. Configure Interface Settings 3. Enable Cloud VPN 4. Configure Business Policy 5. Configure Firewall 6. Review Profile Overview *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-8C960BF4-AE88-4C9D-9750-FA96FBA1C0F3.html

Claims	Exemplary Infringement Evidence
	 *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-2CA50320-D08E-493E-B7EA-5DBAB441BAD4.html

Quick Start Internet

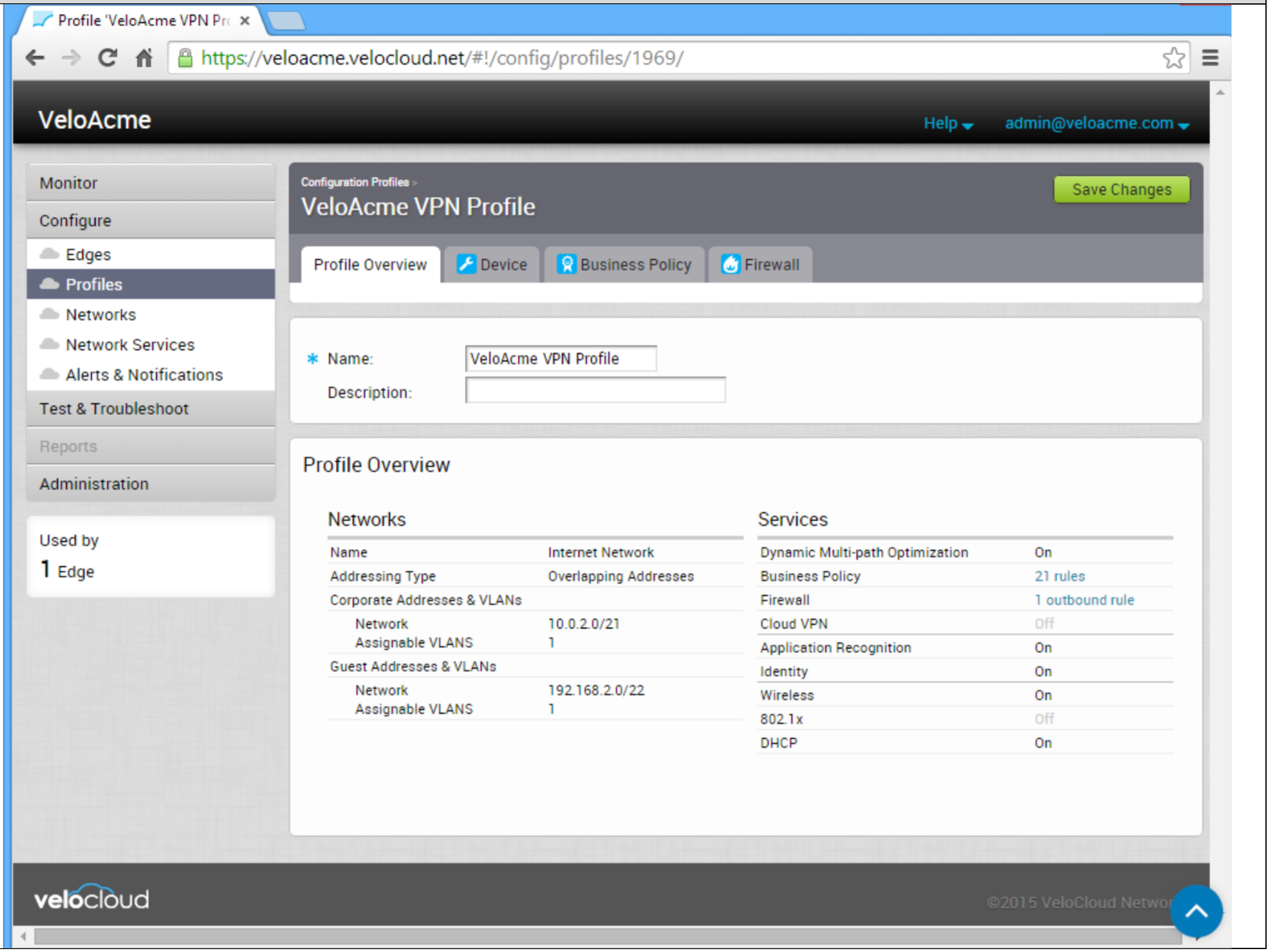
Firewall Status: On

Firewall Logging: On

Used By
0 Edges

Outbound Firewall Rules

		Match			Action
☐	Rule	Source	Destination	Application	Action
☑	1 Acme Outbound Rule 2	MAC: 00:0c:29:54:9a:01	Any	Any	Allow and Log
☐	2 Acme Outbound Rule 1	MAC: 00:0c:29:78:da:f8	Any	Any	Allow and Log

Claims	Exemplary Infringement Evidence
	

VeloAcme VPN Profile

* Name: VeloAcme VPN Profile

Description:

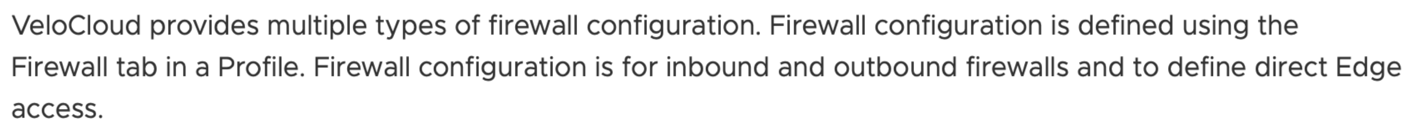
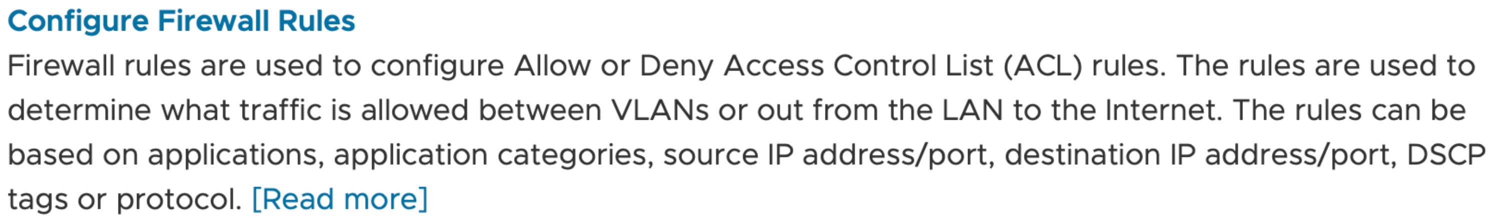
Profile Overview

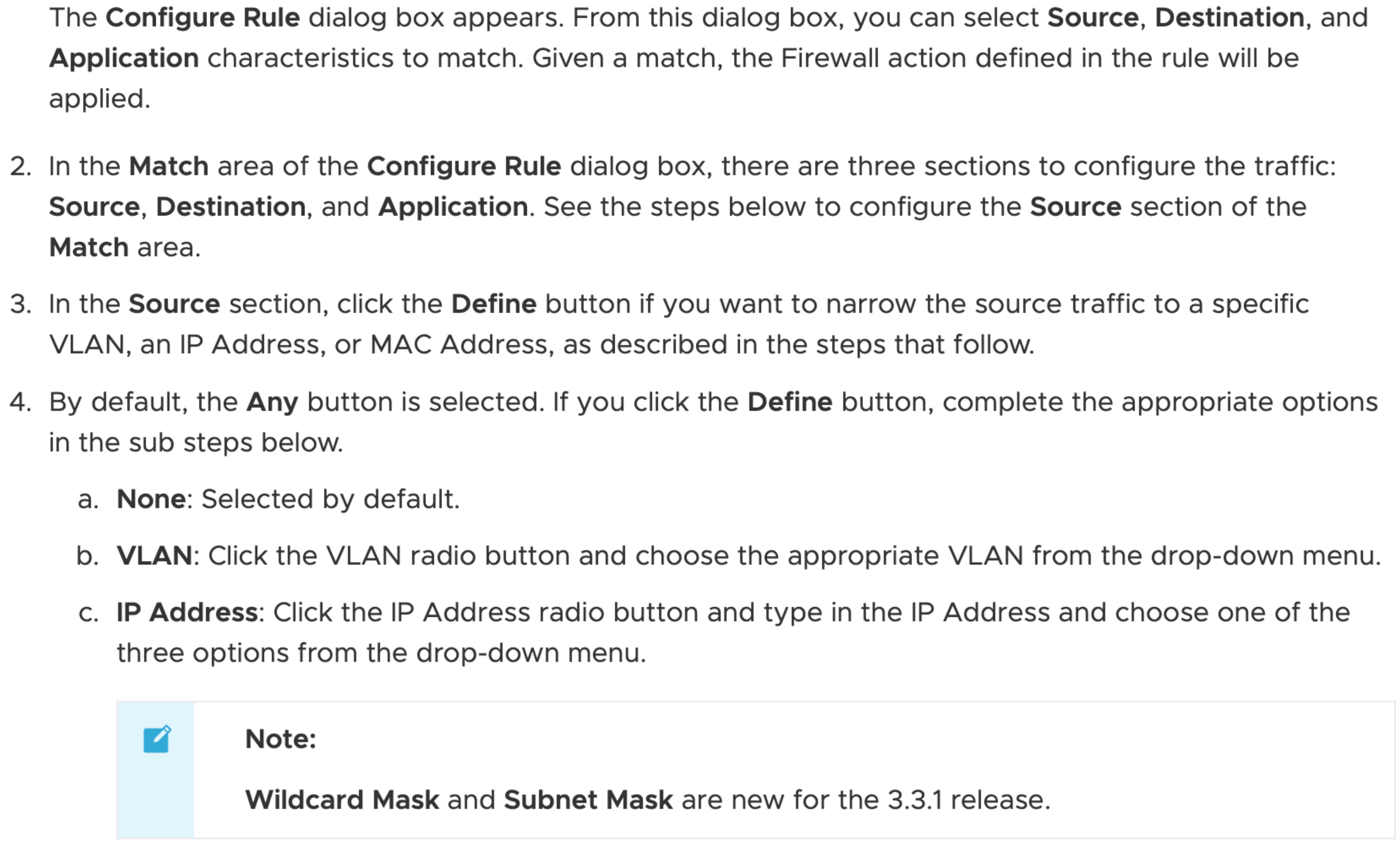
Networks

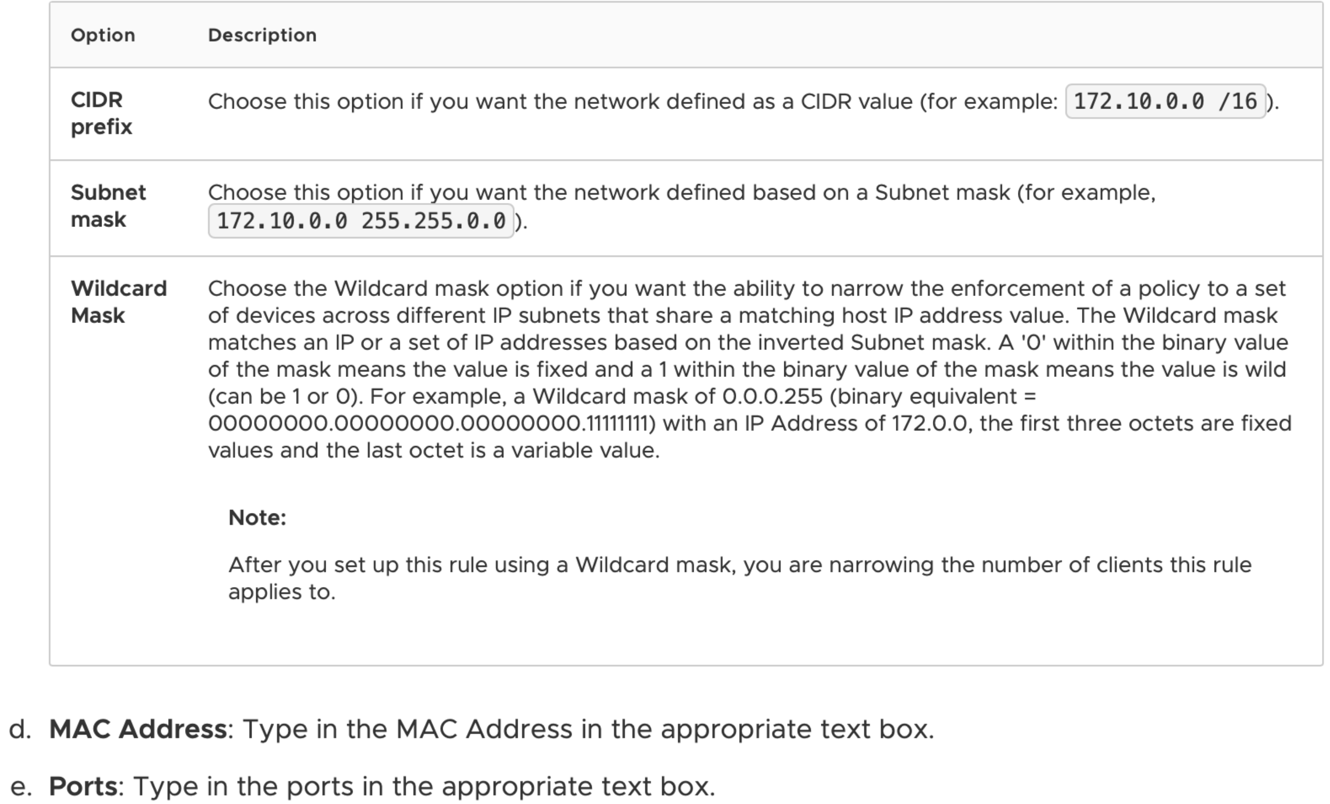
Name	Internet Network
Addressing Type	Overlapping Addresses
Corporate Addresses & VLANs	
Network Assignable VLANS	10.0.2.0/21 1
Guest Addresses & VLANs	
Network Assignable VLANS	192.168.2.0/22 1

Services

Dynamic Multi-path Optimization	On
Business Policy	21 rules
Firewall	1 outbound rule
Cloud VPN	Off
Application Recognition	On
Identity	On
Wireless	On
802.1x	Off
DHCP	On

Claims	Exemplary Infringement Evidence
	See https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-8C960BF4-AE88-4C9D-9750-FA96FBA1C0F3.html  VeloCloud provides multiple types of firewall configuration. Firewall configuration is defined using the Firewall tab in a Profile. Firewall configuration is for inbound and outbound firewalls and to define direct Edge access. *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-AD64ABD4-4388-4CCD-BC16-E993C82817CC.html  **Configure Firewall Rules** Firewall rules are used to configure Allow or Deny Access Control List (ACL) rules. The rules are used to determine what traffic is allowed between VLANs or out from the LAN to the Internet. The rules can be based on applications, application categories, source IP address/port, destination IP address/port, DSCP tags or protocol. [Read more] *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-AD64ABD4-4388-4CCD-BC16-E993C82817CC.html

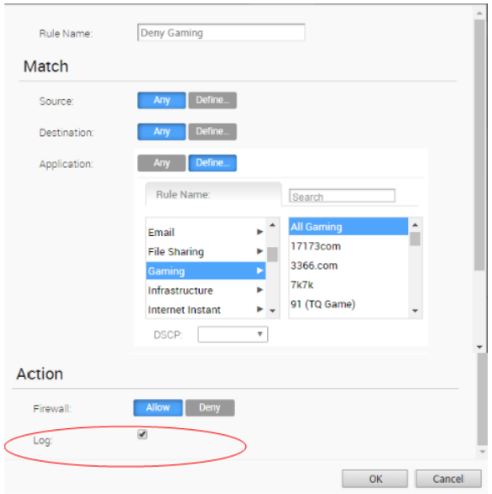
Claims	Exemplary Infringement Evidence
	 The **Configure Rule** dialog box appears. From this dialog box, you can select **Source**, **Destination**, and **Application** characteristics to match. Given a match, the Firewall action defined in the rule will be applied. 2. In the **Match** area of the **Configure Rule** dialog box, there are three sections to configure the traffic: **Source**, **Destination**, and **Application**. See the steps below to configure the **Source** section of the **Match** area. 3. In the **Source** section, click the **Define** button if you want to narrow the source traffic to a specific VLAN, an IP Address, or MAC Address, as described in the steps that follow. 4. By default, the **Any** button is selected. If you click the **Define** button, complete the appropriate options in the sub steps below. a. **None**: Selected by default. b. **VLAN**: Click the VLAN radio button and choose the appropriate VLAN from the drop-down menu. c. **IP Address**: Click the IP Address radio button and type in the IP Address and choose one of the three options from the drop-down menu. **Note:** **Wildcard Mask** and **Subnet Mask** are new for the 3.3.1 release.

Claims	Exemplary Infringement Evidence
	 *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-2CA50320-D08E-493E-B7EA-5DBAB441BAD4.html

Option	Description
CIDR prefix	Choose this option if you want the network defined as a CIDR value (for example: `172.10.0.0 /16`).
Subnet mask	Choose this option if you want the network defined based on a Subnet mask (for example, `172.10.0.0 255.255.0.0`).
Wildcard Mask	Choose the Wildcard mask option if you want the ability to narrow the enforcement of a policy to a set of devices across different IP subnets that share a matching host IP address value. The Wildcard mask matches an IP or a set of IP addresses based on the inverted Subnet mask. A '0' within the binary value of the mask means the value is fixed and a 1 within the binary value of the mask means the value is wild (can be 1 or 0). For example, a Wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111) with an IP Address of 172.0.0, the first three octets are fixed values and the last octet is a variable value. **Note:** After you set up this rule using a Wildcard mask, you are narrowing the number of clients this rule applies to.

d. **MAC Address**: Type in the MAC Address in the appropriate text box.

e. **Ports**: Type in the ports in the appropriate text box.

Claims	Exemplary Infringement Evidence
	Outbound Firewall Rules Click **New Rule** to add a new Firewall rule. The following dialog box appears. Using the dialog box, you can select Source, Destination, and Application characteristics to match. Given a match, the Firewall action defined in the rule will be applied.  Rule Name: Deny Gaming Match Source: Any Define... Destination: Any Define... Application: Any Define... Rule Name: Search Email File Sharing Gaming Infrastructure Internet Instant All Gaming 17173com 3366.com 7k7k 91 (TQ Game) DSCP: Action Firewall: Allow Deny Log: ☑ OK Cancel *See* https://docs.vmware.com/en/VMware-SD-WAN/3.3/VMware-SD-WAN-by-VeloCloud-Administration-Guide/GUID-2CA50320-D08E-493E-B7EA-5DBAB441BAD4.html